Universidade de Brasília – UnB

Faculdade de Direito– FD

A VALIDADE JURÍDICA DAS PROVAS REGISTRADAS EM REDES BLOCKCHAIN NO PROCESSO CIVIL

Jorge Augusto Baars Miranda de Abreu

Orientador: Henrique Araújo Costa

Brasília, 2019

JORGE AUGUSTO BAARS MIRANDA DE ABREU

A VALIDADE JURÍDICA DAS PROVAS REGISTRADAS EM REDES BLOCKCHAIN NO PROCESSO CIVIL

Monografia apresentada à Faculdade de Direito da Universidade de Brasília, como requisito parcial para a obtenção do título de bacharel em Direito, elaborada sob orientação do Professor Doutor Henrique Araújo Costa.

Brasília, 2019

JORGE AUGUSTO BAARS MIRANDA DE ABREU

A VALIDADE JURÍDICA DAS PROVAS REGISTRADAS EM REDES BLOCKCHAIN NO PROCESSO CIVIL

Monografia apresentada à Faculdade de Direito da Universidade de Brasília, como requisito parcial para a obtenção do título de bacharel em Direito, elaborada sob orientação do Professor Doutor Henrique Araújo Costa.

Prof. Doutor Henrique Araújo Costa (Orientador)

_____

Prof. Doutor André Macedo de Oliveira

_____

Prof. Doutor Hércules Alexandre Benício da Costa

_____

AGRADECIMENTOS

Agradeço a Deus e a todos que me acompanharam nessa caminhada para a conclusão de mais uma etapa de minha formação pessoal e profissional, em especial:

À minha esposa, Pricila, que ao longo do curso sempre esteve ao meu lado dando o apoio necessário para superar os desafios de cada dia;

Ao meu querido filho, Rafael, que, antes mesmo de vir ao mundo, trouxe ainda mais alegria e motivação aos meus dias;

Aos meus pais, Silvia e Alceu, pelo carinho, atenção, apoio e exemplo de vida a serem seguidos;

Ao meu irmão, Gui, e aos demais familiares pelo carinho e companheirismo;

Ao Professor Henrique Araújo Costa, pela orientação na elaboração do presente trabalho e pelo conhecimento transmitido sempre que nos encontramos ao longo dessa jornada pelo Direito;

Aos professores André Macedo de Oliveira e Hércules Alexandre Benício da Costa pela gentileza de terem aceitado participar da banca examinadora;

Aos demais professores da UnB, por todos os ensinamentos passados;

Aos amigos do curso de Direito, em especial à Bia, pelos incentivos e pela agradável convivência durante a graduação.

"O Pensamento é o vento, o Conhecimento é a vela, e a humanidade é o navio."

(Augustus Hare)

RESUMO

Este trabalho possui o objetivo de avaliar a validade jurídica das provas registradas em redes blockchain, no âmbito do processo civil Brasileiro. Para tanto, realizou-se uma pesquisa bibliográfica acerca dos possíveis meios de provas utilizados e aceitos no processo civil. Realizou-se uma breve pesquisa sobre o entendimento acerca do tema por outros países, com a finalidade de analisar as melhores práticas. Por fim, foram analisadas as medidas já adotadas pelo Brasil e algumas configurações favoráveis do ordenamento jurídico para aceitar esse meio de prova inovador.

Palavras-chave: Provas. Validade jurídica. Processo Civil. Tecnologia. Direito Digital. Blockchain.

ABSTRACT

This work aims to evaluate the use of blockchain for preserving evidence records in a lawsuit, within the Brazilian civil proceedings. First, it was conducted a brief study on the theme to understand better which kind of evidence means are legally admitted by national courts. Then, it was important to understand how other countries are facing the technology for evidence purpose. Finally, it was essential to comprehend some judicial decisions already taken that indicates that blockchain may be a new mean of evidence in judicial proceedings.

Keywords: Evidence. Legal Validity. Civil Lawsuit. Law and Technology. Blockchain.

LISTA DE ABREVIATURAS E SIGLAS

ICO Initial Coin Offering (Oferta inicial de Moedas)

BCB Banco Central do Brasil

DAO Organizações Autônomas Descentralizadas

PoW Proof-of-Work (prova de trabalho)

PoS Proof-of-Stake (prova de participação)

DPoS Delegated Proof-of-Stake (prova de participação delegada)

LGPD Lei Geral de Proteção de Dados

GDPR General Data Protection Regulation (Regulação Geral de Proteção de Dados)

EU União Europeia

DLT Distributed Ledger Technology

SFD Sistema Financeiro Digital

RTGS Sistema de Compensação em Tempo Real (Real Time Gross Settlement)

DATAPREV Empresa de Tecnologia e Informações da Previdência Social

CPF Cadastro de Pessoa Física

RFB Receita Federal Brasileira

CJF Conselho de Justiça Federal

DBVN Nação Voluntária Descentralizada Sem Fronteiras

ICP Infra-Estrutura de Chaves Públicas Brasileira

SUMÁRIO

INTRODUÇÃO

O Fórum Econômico Mundial[1] estima que, até 2027, 10% do PIB mundial estará relacionado a tecnologia blockchain. Trata-se de uma inovação tecnológica com potencial enorme de ruptura de paradigmas. Sua utilidade é de amplo espectro, desde atividades mais simples, como operações de compra e venda on-line, até aplicações mais complexas que envolvem o registro de imóveis ou de prontuários médicos. São infinitas possibilidades que se abrem no campo do desenvolvimento tecnológico a partir dessas redes. Diante da enorme velocidade de transformação das relações na era da informação e das redes sociais, é imprescindível que o Direito se atualize e que os juristas tenham compreensão das mudanças que afetam diretamente atos e negócios jurídicos diariamente praticados pelos indivíduos.

O Direito já está na era digital há pelo menos duas décadas e nesse curto espaço de tempo já teve que se adequar e se reinventar algumas centenas de vezes. Foi assim com a implantação dos processos judiciais eletrônicos (PJE), que se consolidaram a partir da edição da Lei n º 11.419, de 19 de dezembro de 2006. Acrescente-se, ainda, que a audiência de conciliação e mediação, assim como eventuais intimações, poderão ser realizadas com a utilização do meio eletrônico (arts. 183, § 1º, 334, § 7º, e 1.019, III, CPC/2.015).

Também marca fase da evolução tecnológica no Direito o uso dos certificados digitais, que ficou instituído e formalizado com a Medida Provisória 2.200-2 de 24 de agosto de 2001. Atualmente vivemos um novo capítulo de moedas virtuais e tecnologia blockchain, que requer discussão e aprofundamento de especialistas no tema para eventuais ajustes do ordenamento pátrio.

As inovações tecnológicas impactam diretamente no modo como as pessoas comercializam produtos, como elas prestam serviços e os contratam, bem como uma infinidade de outras situações. Quando as primeiras vendas on-line surgiram, até aquele momento as pessoas não conseguiam dimensionar qual o potencial de sucesso daquela inovação, os riscos associados a essa nova modalidade de comércio e tampouco as novas implicações jurídicas nas relações de consumo e concorrenciais decorrentes da inovação.

[1] http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso em: 29/05/2019

Apoiando-nos na lição da Professora Cristie Ford (FORD, 2017), que estuda a regulação da inovação, com ênfase em inovações financeiras, entendemos que os riscos desconhecidos de inovações financeiras podem colapsar todo o sistema. Segundo a autora, "enquanto a inovação pode criar ambientes de mercado mais eficientes para determinados períodos de tempo, por outro lado também aumenta os riscos, os tornam mais difíceis para serem rastreados e ameaçam a estabilidade sistêmica".

Ao mesmo tempo que a inovação traz um ganho de eficiência e escalabilidade e pode reduzir custos, por outro lado pode aumentar os riscos que ainda são desconhecidos. E esses riscos, se não analisados em tempo, podem comprometer todo o bom funcionamento do sistema. Ela explica, ainda, que a inovação é responsável pelo mercado passar a atuar de forma sistêmica, reduzindo as barreiras entre cada agente do mercado e, dessa forma, os expondo a mais a um risco sistêmico.

> Os sistemas são caracterizados por interconexões, imprevisibilidade e transações dinâmica. O comportamento dos mercados como sistemas resultam das inovações financeiras, que quebram as antigas barreiras entre bancos, companhias de seguro, emissores de títulos e participantes de mercado que operam no mercado de capitais (FORD, 2017)

O grande desafio dos reguladores de Mercado e agências governamentais é não deixar passar despercebido inovações que podem gerar novas relações entre as instituições que estarão descobertas pela legislação e eventualmente colocarão em risco o mercado.

> As inovações têm alterado as relações entre as instituições, investidores e participantes do mercado, introduzindo camadas de complexidade e interconexão. Novas cadeias complexas de instituições e relações podem acabar driblando as exigências prudenciais regulatórias e contornado as formas de regulação tradicionais (FORD, 2017)

O objetivo deste trabalho, portanto, é analisar a possibilidade jurídica da utilização de provas oriundas de registros em rede blockchain nos processos judiciais. Muito tem sido discutido sobre a necessidade ou não de regulação das criptomoedas e sobre o arcabouço normativo que afeta as fintechs e outras aplicações que utilizam as redes blockchain.

Uma das possíveis utilidades dessa tecnologia de rede distribuída é o registro de informações com a finalidade de conferir autenticidade a documentos e dados. Mais adiante, esse registro, que é público e amplamente validado pelos usuários da rede, poderá ser utilizado como meio de prova em um processo judicial. Seria o caso, por exemplo, de registrar na rede

de blockchain um contrato de aluguel de imóvel, que passaria a ter fé pública e, em eventual disputa judicial, serviria de prova em favor das partes.

A fim de entender melhor as possibilidades jurídicas desse tipo de solução em blockchain, o trabalho será iniciado com uma breve revisão da literatura acerca da tecnologia blockchain, suas características e implicações no ordenamento jurídico.

Em seguida, serão observados como outros países têm tratado essa questão e analisados alguns casos de uso e legislações já em vigor que foram recentemente alteradas para contemplar essas inovações tecnológicas.

Pretende-se ainda pesquisar a jurisprudência brasileira acerca do tema para identificar se essas novas modalidades de prova registradas em redes distribuídas já estão sendo debatidas nos tribunais. Por fim, será realizada uma verificação acerca da legislação Brasileira para entender a possibilidade de uso desses novos meios de prova.

1 BLOCKCHAIN

A tecnologia blockchain é uma solução computacional de armazenamento e processamento de informações de forma encadeada e distribuída. Pode-se dizer que o blockchain é uma espécie do gênero conhecido por DLT (Distributed Ledger Technology), que consiste em uma rede distribuída de armazenamento.

De acordo com a definição de Malekan (MALEKAN, 2018), o blockchain combina múltiplas tecnologias, entre elas criptografia e conexão peer-to-peer, e garante que um arquivo ou qualquer dado digital exista em único lugar:

> A definição mais simples de blockchain é uma tecnologia que permite que alguma coisa digital exista em apenas um único lugar. Imagine se alguém pudesse "baixar" um arquivo de música e pudesse ouví-la com toda a conveniência da tecnologia digital, mas com uma diferença: No momento em que o arquivo é enviado a alguém o arquivo torna-se inacessível para aquele que o possuía e o transferiu. O blockchain possibilita soluções como essa pois combina múltiplas tecnologias, desde criptografia até transferências peer-to-peer, para formar uma rede descentralizada e distribuída entre quem possui ou acessa alguma coisa em algum momento na rede. (MALEKAN, 2018)

Existem três arquiteturas de redes básicas que precisam ser compreendidas: redes centralizadas, descentralizadas e distribuídas. Tradicionalmente, os bancos de dados, ou mesmo simples aplicações computacionais, são localizados fisicamente em um servidor central, que concentra toda a gestão dos dados que serão armazenados ou processados. Toda a confiabilidade da rede está concentrada em apenas uma entidade.

Nos bancos de dados descentralizados, o administrador é o responsável pelas funções de atualização e consistência dos dados entre as múltiplas cópias desse livro razão. De forma didática, é como se o administrador do banco de dados de um supermercado mantivesse uma cópia do livro razão com todos os registros de entrada e saída de estoque sempre atualizada e periodicamente atualizasse as cópias desse livro em posse das filiais. Portanto, uma solução de armazenamento descentralizado ainda depende de um ente central para efetuar a validação dos registros e a replicação das informações.

As redes distribuídas utilizam protocolos e infraestrutura que permitem que computadores espalhados ao redor do mundo possam propor e validar transações e atualizar registros de maneira sincronizada na rede. Com isso, o esforço para invadir ou quebrar a segurança de um

servidor centralizado é muito menor que o esforço necessário para invadir um conjunto de servidores distribuídos (DLT).

De outra forma, os novos sistemas baseados em redes distribuídas (DLT) são desenvolvidos para não precisar de uma entidade central de administração desse banco de dados. O Bitcoin, por exemplo, mantém uma base distribuída em que o procedimento de validação das transações é baseado no método de consenso e assinatura criptografada. As transações são conduzidas diretamente entre as partes (peer-to-peer) e depois replicadas para todos os participantes da rede que vão validar esses novos registros em blocos.

Assim, é possível que transações sejam executadas peer-to-peer, sem a necessidade de um intermediário, e os registros das transações são armazenados em um banco de dados distribuído entre todos os participantes dessa rede. Cada integrante dessa rede também possui uma cópia do livro de registro desses blocos. Uma eventual tentativa de hackear a rede e fraudar os dados (roubar moedas, por exemplo) é impossível diante do imenso esforço computacional que seria demandado para invadir e atualizar simultaneamente todas as cópias desse livro razão em cada participante da rede.

Em 2008, com a criação e lançamento do Bitcoin, criptomoeda desenvolvida sobre uma plataforma de blockchain por Nakamoto, essa tecnologia passou a chamar atenção do mundo. Não só pela possibilidade da criação de moedas criptografadas, mas pela extensa gama de soluções que podem ser desenvolvidas utilizando-se a tecnologia.

Nessa linha temos, além das criptomoedas (Bitcoin, Maker, Mixin, Ethereum, Litecoin, Dash etc.), os Smart Contracts, as Fintechs e diversas outras soluções que estão sendo desenvolvidas com a tecnologia de blockchain.

Bancos Centrais ao redor do mundo estão pesquisando e utilizando, ainda em caráter experimental, o uso de Criptomoedas para sistemas de compensação interbancário ou mesmo como meio de pagamento.

O Sistema Financeiro Digital (SFD) é um projeto que une Banco do Brasil, Caixa, Santander e SICOOB com o intuito de desenvolver uma plataforma de transferências eletrônicas em tempo real, alternativa às tradicionais TED e DOC hoje disponíveis. A solução está sendo implementada em uma rede blockchain que viabiliza o registro das transações e a validação pelas instituições financeiras sem depender de uma *clearing*, para que ocorra a compensação.

Na mesma linha, o projeto Jasper, desenvolvido pelo Banco Central Canadense (Chapman *et al.*, 2017), e o projeto Ubin, pela autoridade monetária de Cingapura (MAS, 2017), simulam um sistema de compensação em tempo real (RTGS) utilizando a plataforma de redes distribuídas. As transações são processadas individualmente e imediatamente.

Os Bancos Centrais terão eventualmente que decidir pela emissão ou não de cirptomoedas, seja destinada para o público em geral ou para os integrantes do sistema financeiro. Terão de considerar não apenas as preferências dos consumidores por privacidade ou ganhos com eficiência, mas também os riscos associados a essa emissão que podem impactar no sistema financeiro, em outros setores da economia e até mesmo nas regras da política monetária.

Os Contratos Inteligentes (Smart Contracts) estão sendo desenvolvidos para diversas finalidades, principalmente com o intuito de eliminar intermediários em transações comerciais, reduzir o problema da confiança para a execução de contratos e distribuir o risco, ao desconcentrar o armazenamento dos dados ao longo da rede.

1.1 CARACTERÍSTICAS DAS REDES BLOCKCHAIN

Para analisar aplicações que utilizam redes blockchain no Direito, é preciso compreender melhor as características dessas redes. Como essa tecnologia é algo relativamente novo, ainda existe uma preocupação sobre confiabilidade e sobre se de fato podem ser plataformas para aplicações de grande porte, tais como a emissão de certidões, validação e registro de documentos etc.

Como o próprio nome revela, uma rede blockchain consiste num conjunto de blocos encadeados. Cada bloco possui uma quantidade de registros das transações que foram executadas na rede em um dado intervalo de tempo. Servidores participantes dessa rede disputam um “desafio” matemático, denominado *proof-of-work*, a fim de ganhar o direito de validar um bloco. Uma vez validado, esse bloco de registros é distribuído para todos os participantes da rede que irão concordar com a validade do novo bloco e adicioná-lo à cadeia de blocos existente.

Essas redes podem ser públicas ou privadas. Em ambos os casos, a segurança da rede decorre da imutabilidade dos registros que foram validados e consolidados em bloco. Para que

o novo bloco seja adicionado à rede, é necessário haver um consenso entre os usuários da rede. A regra de consenso varia para cada tipo de rede existente. Para algumas, exige-se a anuência de 50% dos participantes para a validação do bloco, outras exigem um quantitativo maior, como 80%.

Aparentemente, são essas características de imutabilidade dos registros e consenso para validá-los que torna o blockchain um ambiente mais seguro que outras tecnologias de rede.

O Bitcoin é atualmente a maior rede desenvolvida com o conceito blockchain e vem crescendo desde 2008. De lá pra cá, outras redes vêm se desenvolvendo, ganhando espaço no mercado e incrementando novos atributos. Diante da infinidade de possibilidades de uso da tecnologia, uma tendência é a especialização dessas redes voltadas para nichos de mercado específicos, como por exemplo redes blockchain especificas para soluções bancárias, outras para registros públicos, setor de logística etc.

Alguns dos princípios da Tecnologia blockchain, de acordo com William Mougayar (2017), são i) a comunicação Ponto a Ponto (Peer-to-Peer); ii) a eliminação da terceira parte confiável, iii) e a criação sequencial de transações imodificáveis (com data e hora), mostrando assim a prova de trabalho criptografada.

Embora o conceito fundamental de blocos encadeados seja comum a todas essas redes, alguns atributos que as diferenciam podem ser decisivos para a avaliação de compatibilidade da plataforma com o serviço que se deseja implementar na rede.

1.2 ALGUMAS REDES BLOCKCHAIN

A rede Bitcoin, mais conhecida pela criptomoeda associada, é uma rede pública, acessível por qualquer pessoa que queira executar o código, que é aberto é gratuito. Os participantes não precisam ser identificados para participar da rede, podem dessa forma preservar o anonimato. Os participantes também são livres para entrar e sair da rede a qualquer momento.

Há basicamente três formas de participação nessa rede: usuário, minerador e nó. Os usuários são aqueles que estão interessados em registrar uma transação na rede, podem fazê-lo a partir da execução de alguns comandos pelo próprio computador ou podem contratar o serviço de alguma empresa que ofereça efetuar os registros. Os mineradores são aqueles servidores do

código que efetuam o registro das transações em blocos encadeados. Todos eles possuem uma cópia atualizada do algoritmo da rede bem como a última versão desse grande banco de dados, a cadeia de blocos de transações. São esses os grandes responsáveis pela sobrevivência e pelo sucesso da rede. Validam os blocos em troca de incentivos monetários recebidos em btc (bitcoin). Por fim, os nós são participantes da rede que apenas replicam esse banco de dados, mas não atuam validando novos blocos. É o que Malekan explica:

> Entidades que armazenam os blocos são chamados de nós; entidades que inserem novos blocos na rede são chamadas de mineradores. Ambos escolhem se envolver com o processo e participar na rede por interesses próprios, tanto porque eles desenvolvem uma aplicação e tem interesse nos registros armazenados, quanto pelos incentivos financeiros para manter a rede. (MALEKAN, 2018)

A rede Bitcoin foi desenhada de uma forma que os mineradores competem entre si para a solução de um desafio matemático, popularmente chamado de proof-of-work. Aquele que solucionar mais rápido o problema ganha o direito de efetuar o registro de um novo bloco de transações na rede. Em troca esse minerador é recompensado em bitcoins pelo seu esforço computacional efetuado. Os usuários que estão efetuando as transações também pagam uma tarifa por cada transação e esse valor também é repassado aos mineradores. Assim, todos os mineradores têm um grande incentivo de validarem as transações de forma honesta, pois só a partir da confiança dos usuários na rede é que essas moedas passarão a ter algum valor. Malekan explica que a agenda de inflação desenhada para o Bitcoin é o que atribui à moeda a escassez. As regras foram programadas para que a cada 210 mil novos blocos inseridos na rede o valor da recompensa por um bloco cairia à metade. Com isso estima-se que, em 2140, a rede tenha atingido os 21 milhões de bitcoins a partir de quando a validação de novos blocos não mais seria remunerada. No entanto, os mineradores manteriam seus incentivos de permanecer na rede em razão das tarifas (fees) que recebem por transação dos usuários que utilizam a rede.

> O número de novas moedas que um minerador pode auferir por escrever um novo bloco na rede é reduzido a metade a cada 210 mil blocos, e está configurado para ser zerado após 64 reduções. A fórmula permite que estimemos um total de 21 milhões de bitcoins por volta do ano de 2140. (MALEKAN, 2018)

As regras de consenso de validação dos blocos na rede Bitcoin dependem da aceitação da maioria dos participantes (51%), medido em termos de esforço computacional. Nesse caso, se algum participante possui máquinas que processam o algoritmo computacional representando mais da metade da capacidade de processamento da rede, então esse participante

sozinho terá capacidade de validar os blocos, sem necessidade do aceite dos demais membros da rede.

O artigo seminal da rede Bitcoin, idealizada por Nakamoto conclui que:

> Propusemos um sistema para transações eletrônicas sem depender da confiança. Começamos com a estrutura usual de moedas feitas a partir de assinaturas digitais, que fornece um forte controle de propriedade, mas é incompleta sem uma maneira de evitar gastos duplicados. Para resolver isso, propusemos uma rede *peer-to-peer* usando prova de trabalho para registrar um histórico público de transações que rapidamente se torna impraticável para um invasor mudar se os nós honestos controlarem a maior parte da energia da CPU. A rede é robusta em sua simplicidade não estruturada. Os nós operam simultaneamente com pouca coordenação. Eles não precisam ser identificados, pois as mensagens não são roteadas para nenhum lugar específico e precisam ser entregues apenas com base no melhor esforço. Os nós podem sair e se juntar à rede à vontade, aceitando a cadeia de *proof-of-work* como prova do que aconteceu enquanto estavam fora. Eles votam com seu poder de CPU, expressando sua aceitação de blocos válidos trabalhando em estendê-los e rejeitando blocos inválidos, recusando-se a trabalhar neles. Quaisquer regras e incentivos necessários podem ser aplicados com este mecanismo de consenso. (NAKAMOTO, 2008)

As assinaturas digitais, embora confiram autenticidade às transações, não revelam a identidade de seus usuários. Embora pública, a rede é anônima, o que dificulta eventual responsabilização por fraudes.

Outro detalhe que merece destaque é o fato de as regras do algoritmo e as validações dos blocos dependerem de um consenso em que o voto tem peso pela capacidade de processamento computacional. Dessa forma, aquele participante que for capaz de processar o maior volume de dados é quem pode exercer maior influência na rede. Deixamos de ter um ente central de confiança que armazena os dados e toma decisões sozinho para um sistema em que os mais poderosos computacionalmente poderão ter maior controle. Malekan explica que, no intuito de compensar essa transferência da confiança de entidades e Governo para computadores e códigos, Satoshi propôs um sistema totalmente transparente e público em que todos os usuários poderão fiscalizar as operações, senão vejamos:

> Ao projetar o Bitcoin para ser totalmente descentralizado sem nenhum órgão de governo, Satoshi Nakamoto entendeu que ele estava pedindo aos usuários que dessem um salto de fé. Mudar de um sistema de dinheiro controlado pelos governos para um governado por matemática e código é assustador. Para ajudar a preencher a lacuna, ele propôs total transparência (MALEKAN, 2018)

Outra rede em pleno desenvolvimento é a Hyperledger, que aposta na possibilidade de interconexão das diversas redes desenvolvidas em blockchain. Os desenvolvedores, que contam

com o suporte da Linux Foundation, também defendem o código aberto. Algumas variações da rede estão em funcionamento, tais como Hyperledger Fabric, Grid e Indy, que se voltam para tipos de aplicações específicas.

Assim como a rede Bitcoin, a Hyperledger defende o desenvolvimento em código aberto, o que facilita e aumenta a participação de todos os interessados na rede. A plataforma também é desenvolvida para realizar transações peer-to-peer entre partes que não se conhecem e não possuem uma relação de confiança. Também dispensa a presença de um intermediário para validar as transações, que são validadas por consenso de todos os participantes da rede.

> Os sistemas Blockchain são projetados para permitir transações diretas (*peer-to-peer*) entre as partes que não confiam totalmente umas nas outras ou não confiam em nenhuma autoridade central para validar transações ou resolver disputas. Portanto, é essencial que as partes confiem na tecnologia blockchain. Acreditamos que uma abordagem aberta e colaborativa que convide à participação de todas as partes interessadas é a maneira mais eficaz de criar confiança para as empresas - confiança suficiente para que adotem as tecnologias blockchain de maneira ampla e rápida.[2]

A rede Corda tem a proposta de permitir um volume muito maior de transações diárias que outras redes no mercado. Se diferencia das demais ao permitir mais de um tipo de regra de consenso para validação das transações a depender do tipo de aplicação ou informação que esteja sendo implementada na rede.

> Excepcionalmente, a rede Corda foi projetada para suportar volumes que excedam bilhões de transações diárias em uma única rede. Para isso, a Corda permite uma variedade de serviços de consenso (grupos de validadores) otimizados para diferentes propósitos na mesma rede, inclusive na rede Corda global descrita neste capítulo. (Brown, 2018)

Uma outra diferença significativa em relação às redes Bitcoin e Hyperledger é quanto à identificação das partes envolvidas nas transações. A rede Corda pretende ter um único mapa que relaciona identidades dos usuários da rede com identidades do mundo real. Essa necessidade se deve pelo fato da rede ser utilizada para o gerenciamento de contratos reais entre pessoas e firmas, que requerem, eventualmente, ser identificados para fins de responsabilização, por exemplo.

> A rede Corda gerencia contratos reais entre pessoas reais e empresas. Portanto, precisamos que os usuários saibam que estão realmente negociando com quem eles acham que são. Isso requer que exista um mapeamento exclusivo da identidade do mundo real para a identidade da rede (chave pública). Na verdade, é importante enfatizar que os

[2] https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf

> operadores de redes comerciais são capazes e, de fato, devem verificar independentemente as identidades dos participantes antes admitindo-os em suas redes de negócios. É essa camada extra de verificação que permite que a estrutura de identidade em nível de rede Corda seja a mais leve possível, garantindo a exclusividade dos certificados de identidade. (Brown, 2018)

A rede Ethereum, idealizada por Vitalik Buterin em 2013, possibilita a implementação de contratos inteligentes na rede. São registros parametrizados conforme a vontade das partes e que são executados automaticamente quando da confirmação de algum evento que estava previsto naquele contrato. A rede Ethereum é formada por dois elementos: uma linguagem de programação completa (EtherScript) e uma moeda (Ether). Enquanto o primeiro permite às partes formalizarem vários tipos de contratos inteligentes, o segundo é o elemento essencial de incentivo para a utilização da rede Ethereum, além de poder ser utilizada como um meio de pagamento.

Diferentemente do Bitcoin, que pretende, sobretudo, ser uma moeda e, portanto, torna-se um recurso escasso no mercado, a Ethereum está mais voltada para a implementação desses contratos inteligentes e outras aplicações desenvolvidas na rede desvinculadas de alguma criptomoeda. O mecanismo de recompensa para a mineração dos blocos é similar ao do Bitcoin, mas não há em seu código aquele limite previsto de 21 milhões de moedas que a torna uma moeda escassa.

> A rede Ethereum faz isso construindo o que é essencialmente a última camada fundacional abstrata: um blockchain com uma linguagem de programação integrada, permitindo que qualquer um escreva "*smart contracts*" e aplicativos descentralizados (dapps) onde possam criar suas próprias regras arbitrárias de propriedade, formatos de transação e funções de transição de estado. Uma versão básica do Namecoin pode ser escrita em duas linhas de código, e outros protocolos, como moedas e sistemas de reputação, podem ser construídos em menos de vinte. Contratos inteligentes, "caixas" criptográficas que contêm valor e apenas o desbloqueiam se certas condições forem atendidas, também podem ser construídas em cima da nossa plataforma, com muito mais poder do que o oferecido pelo script Bitcoin por causa dos poderes adicionais. (Buterin, 2013)

Em comum, essas redes se dizem ser supostamente mais seguras, imutáveis e transparentes, o que podemos resumir como sendo o grande diferencial dessas redes em relação a outras arquiteturas de rede até o momento utilizadas.

1.3 ATRIBUTOS DAS REDES BLOCKCHAIN

Passamos a analisar pontualmente cada um desses atributos:

1) Segurança

Em tese, a segurança dessas aplicações em rede blockchain decorre do fato de não dependerem de uma entidade garantidora das transações, como já foi anteriormente dito. A desnecessidade de um ente central controlador e verificador dos dados transfere essa credibilidade e confiança para toda a rede de forma distribuída. Assim, só podemos afirmar que a rede é segura se a maioria dos participantes, em termos de capacidade de processamento de dados, forem confiáveis.

O fundador do Bitcoin (NAKAMOTO, 2008) explica que se a maioria da capacidade de processamento é controlada por participantes honestos, a cadeia de blocos "honestos" vai crescer mais rápido que outras cadeias de blocos que porventura estejam sendo geradas por participantes "desonestos". Para modificar um bloco que já foi validado, um indivíduo teria de resolver o *proof-of-work* daquele bloco e de todos os demais que o sucedem e ultrapassar a capacidade de processamento de blocos válidos pelo resto da rede. Conforme novos blocos são adicionados à rede, essa probabilidade de ataque ou modificação de uma transação já registrada em um bloco diminui exponencialmente. O incentivo (o pagamento em bitcoins) ajuda a manter a rede "honesta". Se um hacker detém a capacidade computacional de processamento maior que a de todos os participantes honestos da rede, então ele terá de optar entre alterar as transações que já ocorreram, transferindo bitcoins para ele mesmo ou produzir uma nova moeda, já que ele tem capacidade de consenso. Como é mais lucrativo continuar jogando segundo as regras que já estão estabelecidas, ele irá optar por fraudar as transações, porém a concentração dessa moeda em um participante vai minar o sistema e perder valor a ponto de perder o sentido em realizar esse tipo de ataque.

2) Imutabilidade

A imutabilidade está diretamente relacionada a segurança, quanto mais blocos são validados e encadeados na rede, mais difícil se torna a alteração de um registro que ficou para trás. O participante que desejar alterar uma transação que já foi validada deverá ser capaz de

resolver o desafio matemático *proof-of-work* daquele bloco especifico que contém a transação e todos os demais que tiverem sido encadeados depois.

Pode-se concluir que a característica de imutabilidade da rede blockchain não é absoluta, mas sim dependente do tamanho da rede, da quantidade de blocos que são validados a cada intervalo de tempo, da dificuldade do desafio matemático *proof-of-work*, bem como da quantidade de blocos que já foram encadeados após aquele que se deseja modificar.

Alterar transações de blocos recém-criados é muito mais fácil e requer menos capacidade de processamento que para alterar blocos que foram criados há mais tempo. Da mesma forma, é mais fácil alterar blocos em uma rede com menos participantes que em redes que já possuem centenas ou milhares de nós. Redes que possuem desafios *proof-of-work* mais fáceis ao mesmo tempo que viabilizam a inserção de mais dados por segundo também ficam mais suscetíveis a alterações dos dados recentemente acrescentados.

> Uma vez que o esforço da CPU tenha sido gasto para satisfazer a "*proof-of-work*", o bloco não pode ser alterado sem refazer todo o trabalho. Como os blocos posteriores são encadeados, o trabalho para mudar o bloco incluiria refazer todos os blocos depois disso. (NAKAMOTO, 2008)

3) Transparência

A transparência não se confunde com violação à privacidade nas redes blockchain. São essencialmente transparentes pelo fato de todo novo bloco de transações validado ser replicado para todos os demais participantes da rede indiscriminadamente. Mas, como a informação que está registrada naquele bloco é criptografada, os participantes não têm acesso ao conteúdo. É como se pudessem validar os requisitos formais de um pacote dos correios sem acesso ao conteúdo que está sendo transmitido. Só abrirá a correspondência o participante que possuir a chave única da criptografia.

No modelo tradicional centralizado, a privacidade depende de que apenas as partes envolvidas em uma determinada transação possam ter acesso a ela. Imagine se a cada transferência eletrônica bancária a instituição disparasse um comunicado para todos os clientes informando da transação. É mais ou menos isso que acontece na rede blockchain, mas o conteúdo só estará acessível para as partes que detêm a chave criptográfica.

> O modelo bancário tradicional atinge um nível de privacidade ao limitar o acesso à informação às partes envolvidas e ao terceiro de confiança. A necessidade de anunciar todas as transações exclui publicamente esse método, mas a privacidade ainda pode ser mantida quebrando o fluxo de informações

> em outro lugar: mantendo as chaves públicas anônimas. O público pode ver que alguém está enviando um valor para outra pessoa, mas sem informações vinculando a transação a ninguém. Isso é semelhante ao nível de informações divulgadas pelas bolsas de valores, onde o tempo e o tamanho dos negócios individuais, a "fita", são tornados públicos, mas sem dizer quem eram as partes. (NAKAMOTO, 2008)

O mecanismo de transparência também varia entre os diversos tipos de rede. A rede Corda, por exemplo, propõe um modelo em que há um comitê de participantes, representativo da rede, que é responsável por definir regras de consenso, atualizar parâmetros diversos da rede, estabelecer regras de identificação dos usuários da rede, entre outras atribuições. (HEARN, 2016)

A impossibilidade de identificação dos envolvidos em uma transação, ao passo que preserva o direito de privacidade, também representa uma dificuldade de responsabilização por alguma falha na transação. É o que aponta o professor Ross Buckley:

> Todas as transações em blockchains abertos (não autorizados) são públicas. Isso não significa que esteja sempre claro quem executou as transações em um blockchain público. No blockchain do Bitcoin, por exemplo, todos os usuários têm uma chave pública e não há como determinar quem está por trás de uma chave. Também não é possível determinar quem está por trás de uma conta específica através de uma organização central, porque nenhuma organização central regula a blockchain do Bitcoin. Na prática, isso pode levar a problemas. Se você não sabe com quem está negociando em uma blockchain, é praticamente impossível levar a parte à corte se algo der errado com a transação. É concebível, por exemplo, que você faça um pagamento com Bitcoin e acidentalmente insira um zero adicional, o que significa que dez vezes mais Bitcoins como pretendido são transferidos para a parte receptora. Se tal transação tivesse ocorrido através de um banco, seria relativamente simples descobrir a identidade da parte receptora e forçar o reembolso judicialmente. Para uma transação blockchain, descobrir a identidade da parte receptora é simplesmente muito mais complicado. (ZETZSCHE, BUCKLEY, ARNER, 2018)

Na compreensão de De Filippi e Wright (DE FILIPPI, WRIGHT, 2018), uma rede blockchain é um banco de dados transparente e sequencialmente organizado que se torna resiliente e resistente a mudanças e adulterações. Os registros armazenados na rede são distribuídos para os participantes, que se comunicam ponto a ponto (peer-to-peer). Uma vez que a informação é registrada na rede, fica muito difícil apagar ou modificar essa informação sem que se tenha um custo muito elevado. Como toda transação realizada na rede blockchain é transparente e digitalmente assinada, é sempre possível avaliar, com alta probabilidade, se os dados foram originados de uma conta particular. Nota-se que diante de uma infinidade de aplicações para a tecnologia blockchain, é difícil que uma mesma arquitetura funcione

igualmente bem para todas as finalidades. Por essa razão a tecnologia se adapta e surgem variações de redes que podem ser:

a) Públicas ou Privadas
b) Com ou sem permissão
c) Utilizar métodos distintos de criptografia
d) Utilizar diferentes regras de consenso

Cada arquitetura levará em conta o que é mais relevante para a aplicação desejada. Se acessibilidade à rede é mais importante que tempo de processamento, por exemplo, então pode ser que a rede prefira ser publica sem permissão e com um mecanismo de criptografia mais severo, ou uma regra de consenso mais rígida. Por outro lado, se a rede é privada e não requer tanta preocupação com o sigilo das informações, então poderá aumentar a eficiência de processamento estabelecendo uma regra de consenso mais branda.

O dilema entre transparência e anonimato é elucidado por Malekan:

> Os *trade-offs* entre transparência e anonimato existem em um espectro, e cabe a cada usuário, bem como a nossa sociedade como um todo, decidir onde nesse espectro eles gostariam que seu dinheiro estivesse. Felizmente, é fácil tomar uma decisão informada sobre os atributos de um blockchain. Quase tudo no espaço da criptomoeda é de código aberto, o que significa que qualquer pessoa pode espiar para ver como o software subjacente funciona. Assim como a verificação de cada transação é distribuída, também é a verificação dos recursos de uma criptomoeda. (MALEKAN, 2018)

1.4 RISCOS E AMEAÇAS ASSOCIADOS ÀS REDES BLOCKCHAIN

Para avançar, precisamos verificar alguns pontos mais sensíveis dessas redes, que eventualmente podem representar um risco de falha de operação e comprometer todos os usuários de um desses serviços desenvolvidos em uma rede blockchain.

Software e Criptografia

O software que implementa uma rede blockchain pode ser desenvolvido por qualquer programador e esse código pode possuir falhas que só venham a ser identificadas depois que a rede estiver em operação.

A linguagem de programação utilizada para o desenvolvimento desse script também pode ser qualquer uma, desde as mais conhecidas C++, Java, como outras mais restritas. A

confiabilidade da rede, portanto, dependerá do software e da linguagem em que foi desenvolvida.

Quanto à criptografia, atualmente existem diversos algoritmos, uns mais testados e eficientes que outros. Se uma rede é implementada com um método de criptografia fraco, então estará naturalmente mais vulnerável que outra rede similar que utilize um algoritmo criptográfico mais complexo.

A rede Bitcoin, por exemplo, usa o algoritmo SHA-256 testado para *hashing*. Mas estudos mostraram que a computação quântica acabará por levar esse algoritmo a ser quebrado. Outros tipos de blockchain estão implementando novos algoritmos criptográficos onde tudo o que se tem é a garantia do desenvolvedor de que funciona[3].

Continuidade da Rede

O problema da confiança no armazenamento das informações é um ponto crítico nas redes blockchain. As informações dependem de os mineradores estarem rodando o script de validação de blocos constantemente. Se por alguma razão esses servidores param de atuar e não rodam mais o protocolo, então o sistema pode ruir, embora as informações permaneçam públicas e disponíveis a todos que tem acesso a rede e mantem uma cópia do banco de dados. O Bitcoin, por exemplo, utiliza o método de incentivos, por meio da mineração, para que sua rede esteja sempre em execução e crescimento, garantindo que as transações sejam sempre validadas. Porém, é difícil prever se por alguma falha de código ou mesmo por desinteresse dos usuários essas redes continuarão ativas por tempo indeterminado.

Em um cenário de desuso da rede, os mineradores teriam menos interesse em continuar suas atividades, a moeda perderia valor e eventualmente essa rede seria descontinuada. Para as aplicações e soluções desenvolvidas sobre essas plataformas e que dependam da garantia de continuidade das redes, essa é uma preocupação que ainda permanece.

Associada a essa questão, estão as atualizações do algoritmo da rede que também acontecem mediante o consenso dos mineradores. Não havendo unanimidade, por exemplo, é possível que parte dos mineradores sigam a construção desses blocos de informações com regras de validação diferentes dos demais mineradores. Isso é o que se chama de modo simplista de *fork*, justamente por ser uma bifurcação da rede. É um ponto a partir do qual duas novas

[3] MEARLAN, 2008

redes se formam e passam a viver de formas independentes. Apenas compartilham todo o histórico de blocos até o momento do *fork*. Isso pode ser um problema de falta de continuidade para algumas aplicações que dependam de um histórico único dos registros na rede.

Confiabilidade da rede e dos dados

As redes blockchain supostamente resolvem o problema da falta de confiança de armazenamento, uma vez que os conjuntos de dados armazenados são validados por cada nó integrante dessa rede. Essa tecnologia de armazenamento pode assegurar de forma mais eficiente que os dados armazenados não sejam manipulados. Outra garantia que a rede possibilita é que cada transação terá uma assinatura (uma chave privada criptográfica) referente ao autor da transação, impossibilitando a duplicidade de transações (o problema do *double-spending*).

Em contrapartida, apesar dessas proteções inerentes às redes, um dado incorreto que é armazenado na rede não pode ser corrigido. Embora a imutabilidade seja um mecanismo de proteção da rede, por outro lado ela pode gerar um "lixo", uma quantidade de informações registradas na rede, que não precisavam estar lá. O mecanismo de validação das transações não garante a veracidade dos dados inseridos, não protege uma distribuição de dados indesejada, nem controla a perda ou manipulação de dados. Essas vulnerabilidades motivam a reflexão sobre a validade jurídica de informações registradas nesse tipo de rede.

Privacidade de dados

Enquanto a transparência é uma das características dessas redes, que minimiza o problema da confiança e as tornam mais transparentes, o excesso de transparência pode resultar em uma disseminação ou compartilhamento de informações indesejadas, falsas ou imprecisas, que foram inseridas no sistema indevidamente. O fato de a tecnologia não possibilitar que dados sejam apagados da rede agrava mais ainda esse problema se dados privados forem disseminados. O Direito de Esquecimento, por exemplo, fica prejudicado e mais difícil se torna a reparação dessa violação.

Essa é uma preocupação do mundo inteiro, que vem no sentido de regulamentar e responsabilizar o uso indevido de dados pessoais. Nessa linha, é o que propõe a Lei Geral de Proteção de Dados, editada no Brasil em agosto de 2018, trata-se da Lei n 13.709/2018. Daí decorre uma outra preocupação, que é a dificuldade de responsabilização em redes distribuídas.

Se não há um ente responsável pela execução do algoritmo e pela replicação do banco de dados, então como responsabilizar a rede pela inserção indevida de dados?

Diferentemente do que vem acontecendo com a responsabilização de empresas, tais como Facebook ou Twitter, pela exposição de dados indesejados, nas redes blockchain não há um órgão central a ser responsabilizado.

Insider trading e abuso de mercado

A divulgação de informações sobre registros de operações de um determinado ente da rede ou o uso de dados da rede para manipular preços, por exemplo, podem aumentar os riscos legais dessas redes. Embora o conteúdo seja inacessível, é possível identificar que um determinado autor de um conjunto de transações efetuou uma série de registros na rede. Se de alguma forma alguém vincular corretamente o autor a uma pessoa física ou jurídica, então será possível saber que aquela pessoa ou empresa possui um determinado interesse, como, por exemplo, adquirir uma empresa concorrente, ou realizar um empréstimo, ou comprar uma propriedade, a depender do tipo de rede e aplicação em que estiverem transacionando.

Riscos Cibernéticos

Informações registradas de forma imprecisa na rede podem se tornar uma grande ameaça. Os ataques podem direcionar suas energias não a destruição ou quebra de informações dos servidores que armazenam os blocos, mas sim em etapa anterior que gera a transação. Imagine que, ao realizarem uma transação entre dois bancos trocando ativos financeiros, a informação sobre essa operação seja violada e registrada na rede de forma equivocada. As partes não saberão e toda a rede validará uma informação imprecisa da operação que houve entre as partes. No Bitcoin, por exemplo, o maior risco está nas *Wallets* (Carteiras) que registram o valor que o investidor possui da moeda. São elas os responsáveis pela emissão da chave privada para cada usuário, que deverá guardá-la em segurança sob pena de ter suas moedas roubadas ou inacessíveis. Se o cyber ataque for direcionado a essas entidades (*wallets*) o risco de fraude é muito maior que o risco de ataque à rede propriamente dita.

Ataques de Força Bruta

Para um ataque a uma rede blockchain, é necessário um aporte de energia superior a 51% de toda a energia da rede. Isso porque cada nó da rede tem um consumo de energia e um processamento dos dados da rede. Para enganar a rede e convencer os nós a processarem

informações falsas ou atualizarem o software com uma alteração maléfica e danosa ao sistema, o ataque precisa interferir em muitos nós simultaneamente.

Nas redes blockchain, os nós não são nem igualmente importantes e nem igualmente seguros, isso porque a rede trabalha com incentivos. Haverá nós processando uma quantidade de dados muito maior que outros nós a depender de sua capacidade de processamento computacional.

Com isso, os nós têm tamanhos diferentes e logo pesos diferentes nessa equação. Da mesma forma, alguns nós terão sistemas de segurança mais fortes que outros e, portanto, haverá diferenciação entre os nós quanto a esse quesito.

> The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes. (NAKAMOTO, 2008)

Double spending

O problema do *double spendig* (duplicidade de pagamento) consiste na emissão de uma unidade da moeda (ou uma transação qualquer) para dois usuários simultaneamente. Mecanismos de controle estão constantemente atentos a possíveis registros/criação de novas moedas. Se eventualmente houver um registro falso ou errado, os nós irão interromper a geração de novas moedas ou de qualquer outro registro. A depender do tempo em que o serviço fique "desligado" pode haver uma significativa queda do valor financeiro da moeda. Um dos tipos de ataque à rede são os DDOS, que consistem em ataques de distribuição de negação de serviço.

A solução do problema de *double-spending* pode ser feita da seguinte maneira: Se uma mesma transação for enviada duas vezes para a rede, então apenas a última transação será válida e a primeira será desconsiderada. Nos modelos de rede centralizada, a entidade central (como o banco, por exemplo) era responsável por verificar cada transação para saber se houve uma duplicidade. No modelo distribuído proposto pelo Bitcoin, em que não há a entidade verificadora, é preciso que os participantes da rede concordem com apenas uma ordem cronológica de recebimento das transações. O participante que efetuou a transação requer uma confirmação de que a maioria dos participantes da rede concordaram que aquela transação foi a primeira recebida.

Um participante desonesto, exemplifica (SCHWATRZ, YOUNGS, BRITTO, 2014), poderia realizar duas transferências na rede com recursos em sua conta para cobrir as despesas de apenas uma transferência. As transações individualmente estão corretas, mas se forem

executadas simultaneamente e a rede não tiver conhecimento da duplicidade, então estaríamos diante de um problema (o *double-spending*).

Escalabilidade

Uma das principais questões suscitadas pelos usuários das redes blockchain é quanto à capacidade de efetuar grande quantidade de registros na rede em um curto espaço de tempo. Diferentemente de soluções que adotam um banco de dados centralizado ou mesmo descentralizado, mas que não dependem de um processo lento de validação das transações, as redes blockchain são projetadas para que esse tempo seja mais lento.

A necessidade de solução do PoW por parte dos mineradores impõe um tempo médio de 10 minutos para que cada novo bloco seja inserido na rede Bitcoin, por exemplo. Outras redes ajustaram esses parâmetros para permitir uma inserção de novos blocos de maneira mais ágil, porém, à medida que se reduz a necessidade de esforço computacional, pode-se colocar a honestidade da rede em cheque.

Atualmente, o bitcoin consegue processar cerca de 7 transações por segundo. A rede Ethereum, o segundo maior projeto de criptomoeda e blockchain do mundo, está atualmente trabalhando no escalonamento de sua plataforma para processar 1 milhão de transações por segundo a partir do atual máximo de transações de 15.000 por segundo.

Comparativamente, a VISA processa cerca de 2.000 transações por segundo e as bolsas de valores executam 80.000 transações por segundo. A rede Bitcoin também tem trabalhado com o Lightning Protocol no sentido de ampliar a capacidade de processamento. Com esse protocolo, a rede pode processar um limite de 60.000 transações por segundo, viabilizando a implementação de projetos comerciais que demandam essa escalabilidade.

Conforme Mougayar (2017), o blockchain não é um banco de dados eficiente para armazenamento de muitas informações, como grandes bases de dados de cadastro por exemplo, pois a criptografia utilizada por esse tipo de rede proporciona uma lentidão nos processos, assim, basicamente aparecerão aplicações híbridas, nas quais softwares dotados de bancos de dados utilizarão, em cada registro armazenado nesses bancos de dados, uma validação através da tecnologia blockchain.

Associado ainda ao problema da escalabilidade está o tamanho dos blocos. A rede Bitcoin trabalha com blocos de tamanho máximo de 1 Mega Byte. Em situações de alto volume

de transações, surge uma fila de transações a espera de novos blocos para serem registrados na rede. Se de um lado o tamanho do bloco menor possibilita a participação de mais nós na rede mantendo esse banco de dados distribuído, de outro retira a capacidade de processar um volume maior de transações por bloco. Em 2017, um grupo de mineradores da rede Bitcoin, favoráveis a uma alteração do tamanho do bloco, promoveram um *hard fork* na rede, que originou a Bitcoin Cash, que atualmente trabalha com blocos de 2 a 4 megabytes.

Os desenvolvedores de redes blockchain encaram um dilema, segundo Song (SONG, 2018): para utilizar o máximo potencial da tecnologia precisam aumentar a escalabilidade e a maioria dos participantes deve estar de acordo com a estratégia. Para ter sucesso, os defensores devem estimular o interesse do mercado na tecnologia, mostrando que os benefícios compensam os investimentos.

Risco Operacional

Aqui estão associados os riscos de um código sem manutenção, desatualizado ou atualizado de forma enviesada e benéfica a alguém ou a alguma parte da rede. As atualizações e as melhorias do sistema dependem de desenvolvimento humano e decisão de um grupo de pessoas da rede que acabam por representar o mesmo risco do ente regulador centralizado (o banco central, por exemplo).

Outra questão aqui é a possibilidade de um usuário transferir um valor em moeda virtual para o destino errado. Uma vez realizada a operação, não há volta, não há direito de reivindicar uma correção dessa informação na rede.

No intuito de contingenciar o risco operacional associado ao negócio desenvolvido na rede, poderia haver um conjunto de regras que instituísse limites e regras prudenciais de operação. Um exemplo disso é Basileia 3, que estabelece regras que norteiam as instituições financeiras, que devem manter uma infraestrutura adequada, controle das perdas e um capital de contingência.

Para as moedas virtuais desenvolvidas sobre uma rede blockchain, por exemplo, pode-se exigir dos participantes alguns compromissos, como adesão a um seguro, capital mínimo, ou mesmo impor um limite de volume negociado com a mesma contraparte.

Risco Sistêmico

O risco sistêmico é aquele que ameaça o funcionamento da rede como um todo. Certas ocorrências que podem destruir todo o sistema e atingir terceiros que não fazem parte da rede. O risco não está mais limitado a um componente dessa rede e sim ao todo.

Os autores De Filippi e Wright (DE FILIPPI, WRIGHT, 2018) elencam uma série de possíveis riscos associados às soluções Governamentais desenvolvidas em redes blockchain. Aplicações de registros imobiliários em um país como os EUA, por exemplo, poderiam ser violadas por outros países ou terceiros que tivessem uma capacidade computacional maior que a da rede utilizada pelo sistema; a perda ou roubo das chaves privadas de autenticação das transações também poria em risco todo o sistema; as redes blockchain, como já foi dito, não garantem a qualidade e acurácia dos dados armazenados; registros inseridos equivocadamente permaneceriam na rede para sempre. Segundo os autores, existe um "cemitério" de iniciativas privadas de sistemas de registros públicos que não tiveram o suporte do Governo e não conseguiram avançar na implementação dos serviços. Sem leis ou regulamentos Governamentais que obriguem a utilização desses serviços, as informações ficarão incompletas na rede e a solução estará fadada ao fracasso.

1.5 APLICAÇÕES EM REDES BLOCKCHAIN

A cada dia mais aplicações são desenvolvidas utilizando as mais diversas redes blockchain existentes no mundo. Estatísticas apontadas no relatório trimestral da ICOBENCH mostram que foram mais de 300 lançamentos de novas soluções ICO (*Initial Coin Offerings*) só no primeiro trimestre de 2019.[4] Nesse grupo estão não apenas as famosas criptomoedas, mas novas plataformas, aplicações voltadas para o setor financeiro, setor imobiliário, setor hospitalar, logística etc.A rede blockchain mais utilizada para o desenvolvimento dessas novas soluções é a Ethereum. De um total de 5.012 aplicações, 4.422 foram desenvolvidas sob a plataforma Ethereum, 122 utilizaram a rede Waves e apenas 25 utilizam a rede Bitcoin, até o final do primeiro trimestre de 2019, conforme aponta o relatório.

As aplicações mais frequentemente desenvolvidas são novas criptomoedas e novas plataformas. No entanto, as soluções voltadas para Bancos, Big Data e para o mercado

[4] https://icobench.com/report?utm_campaign=im2018report&utm_source=statsandfacts. Acesso em: 20/04/2019.

Imobiliário foram as que mais receberam investimentos somando mais de USD 90 milhões só no primeiro trimestre de 2019.

Segundo dados divulgados pela COINLIB, existem atualmente mais de 5.737 criptomoedas, correspondendo a um valor de mercado de USD 92,97 bilhões (atualizado em 20/04/2019)[5]. Diante desse expressivo número de aplicações que nascem a cada dia utilizando diferentes redes blockchain, deve-se analisar algumas aplicações pertinentes ao tema, mais especificamente as aplicações voltadas para o registro e validação de documentos públicos e autenticidade de informações.

Conforme descrevem De Filippi e Aaron Wright, o potencial de uso dessas redes vai além de pagamentos, finanças e contratos. Aproveitando os atributos de resistência a adulterações e resiliência, as redes podem ser utilizadas para registros públicos e outros mecanismos de autenticação e certificação de informações.

> O potencial de uso dos blockchains vai muito além de seu uso inicial em sistemas de pagamentos, finanças e contratos. Os blockchains estão servindo como um repositório resistente e inviolável para registros públicos e outros tipos de informações autenticadas e certificadas, atraindo a atenção de governos em todo o mundo. (DE FILIPPI, WRIGHT, 2018)

As redes blockchain são vistas como uma nova ferramenta para criar registros governamentais e sistemas de manutenção de registros mais confiáveis e transparentes para modernizar e proteger cada vez mais informações críticas do governo. A tecnologia pode servir como um *backbone* para registros governamentais, fornecendo aos cidadãos acesso à informação sob demanda e usando o dispositivo de sua escolha. Assim como as moedas digitais, esses sistemas podem ser projetados para serem sem fronteiras, servindo como uma infraestrutura comum em todo o mundo.[6]

Em linha do que propõem os referidos autores, algumas iniciativas no Brasil já estão em desenvolvimento. É o caso do projeto desenvolvido pela Empresa de Tecnologia e Informações da Previdência Social – DATAPREV, que lançou em 20/11/2018 uma aplicação em blockchain para troca de informações da base de cadastros dos CPF (Cadastro de Pessoa Física). A aplicação possibilita a troca de informações entre a Receita Federal e mais de 700 entidades

[5] https://coinlib.io/coins. Acesso em: 20/04/2019.
[6] Idem

credenciadas que atualmente acessam esses dados. A solução foi desenvolvida em uma arquitetura de rede blockchain pública com permissionamento. [7]

O projeto é fruto de uma atualização normativa da Receita Federal do Brasil, que editou a Portaria RFB nº 1.788/2018 que autorizou o compartilhamento dessas bases de dados por meio de rede permissionada blockchain. Na visão dos desenvolvedores da aplicação, o processo ficou mais seguro, integrado e eficiente.

O projeto piloto conta com participação do Conselho de Justiça Federal (CJF) e a previsão é de que até julho deste ano diversas entidades de todos os poderes e esferas estejam utilizando a solução para a troca de informações da base de CPFs.

Na Suécia, um grupo de entidades privadas e do governo[8] trabalham juntos no desenvolvimento de uma solução que utiliza uma rede blockchain cuja finalidade é o registro de compra e venda de imóveis. Um processo que hoje é essencialmente manual e feito em papel se tornará mais eficiente, seguro e transparente para todas as partes envolvidas. [9]

A autenticação de existência ou posse de um documento é parte essencial de muitos processos financeiros ou jurídicos. O desafio do modelo tradicional de validação de documentos é a confiança na entidade verificadora, além de aspectos físicos como o armazenamento dos documentos.

A tecnologia blockchain possibilita o desenvolvimento de aplicações alternativas a esse modelo tradicional de autenticação de existência. Nas redes, o usuário só precisa armazenar uma assinatura e um selo de tempo associados ao documento que se pretende armazenar. A validação será realizada pelos participantes da rede de acordo com o procedimento que já foi detalhado anteriormente. Para registrar a propriedade de um ativo, uma transação é criada com referência a um ativo físico. Essa informação é armazenada na rede blockchain com a necessidade de pouquíssimo espaço de memória, e pode ser associada a todo tipo de bens e serviços associados. O proprietário da chave privada daquele registro público é registrado como o proprietário daquele ativo.[10]

[7] https://portal.dataprev.gov.br/dataprev-desenvolve-solucao-com-tecnologia-blockchain-para-compartilhamento-da-base-cpf. Acesso em 20/04/2019.
[8] EVRY, Lantmäteriet (the Swedish Mapping, Cadastral and Land Registration Authority), Landshypotek Bank, SBAB Bank, Telia, ChromaWay and Kairos Future
[9] https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain. Acesso em: 20/04/2019.
[10] https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Acesso em: 27/04/2019.

A empresa Factom desenvolveu uma camada virtual que possibilita a utilização da rede Bitcoin para o desenvolvimento de aplicações não financeiras. Um projeto piloto desenvolvido pela empresa pretende registrar e validar contratos imobiliários em Honduras, que historicamente sofre com a falta de registros territoriais confiáveis, ensejando um alto custo para identificação dos reais proprietários das terras e muitas vezes levando as disputas para a justiça, é o que explicam os autores (SNOW, DEERY, JOHNSTON, KITBY, 2014).

Uma boa ilustração da utilidade de um serviço de registro de propriedade por meio de redes blockchain é trazida por De Filippi e Wright:

> Por exemplo, na Síria, devastada pela guerra, colonos xiitas, apoiados pelo Irã, invadiram o país, reivindicando terras onde antes residiam antigos moradores sunitas. Para evitar que os residentes sunitas deslocados recuperem suas terras, os colonos xiitas incendiaram sistematicamente os cartórios de registro de terras em todo o país. Se a Síria tivesse implementado um registro de terra baseado em blockchain em uma rede amplamente distribuída - como o Bitcoin - antes do conflito entrar em erupção, o incêndio teria tido pouco efeito. Por causa da natureza resiliente de um blockchain, mesmo se as chamas envolvessem o sistema tradicional de registro de terras da Síria - e mesmo se os *data centers* da Síria fossem destruídos - cópias dos registros de propriedade permaneceriam armazenadas com segurança nos computadores de mineradores espalhados pelo mundo que suportam a rede Bitcoin. Como um blockchain é resistente a mudanças, se os colonos xiitas tivessem assumido diretamente o controle da terra Síria e tivessem designado ilegalmente terras para novos residentes xiitas, os sírios deslocados ainda poderiam provar suas reivindicações anteriores de propriedade assim que o conflito diminuísse. Contando com os registros ordenados sequencialmente mantidos na blockchain do Bitcoin, qualquer residente Sírio desalojado poderia usar um blockchain para fundamentar uma ação legal para recuperar suas terras. (DE FILIPPI, WRIGHT, 2018)

O Estado de Delaware, nos EUA, lançou uma iniciativa utilizando rede blockchain para o registro de empresas e participações societárias. O estado americano é conhecido por atrair a fundação de grandes empresas, pelas facilidades legais e burocráticas que oferece. Atualmente, é sede de 66% das 500 empresas mais ricas do país. Também é responsável por sediar 85% das ofertas públicas de ações de empresas que estão abrindo capital na bolsa, segundo dados de divulgados por Stromberg (STROMBERG *et al.*, 2018).

O projeto, que foi iniciado em parceria com a empresa Symbiont e segue com a IBM, depois de algumas alterações de equipe, pretende reduzir o tempo de transferências de ações de empresas, que atualmente dura até 3 dias. Com o uso da rede blockchain, esse tempo pode ser quase instantâneo.

A IBM, em parceria com a startup Proxeus e outras entidades, desenvolveu na Suíça um sistema utilizando as redes Hyperledger ou Ethereum que efetua o registro de empresas nas juntas comerciais. As partes tradicionalmente envolvidas nessa operação passaram a efetuar as validações através da rede. Bancos, empresários, notários, advogados e a junta comercial de registro de empresas gastam muito menos tempo e recursos para completar uma operação de registro.[11]

Na Estônia, a organização Bitnation desenvolveu uma plataforma que oferece uma enorme gama de serviços públicos, entre eles, os notariais, tais como registro de nascimento, casamento, testamentos etc. Bitnation refere-se à primeira iniciativa no Mundo de ser uma Nação Voluntária Descentralizada Sem Fronteiras (DBVN). A organização foi lançada em 2014 por Susanne Tarkowski Tempelhof (TEMPELHOF *et al.*, 2017), que explica que seus serviços criam competitividade e ameaçam Governos Centrais em determinados serviços públicos que hoje não são tão eficientes e muitas vezes são onerosos para o Estado.

A empresa Ubitquity também desenvolveu uma aplicação utilizando o blockchain para o registro e rastreamento de propriedades. Com isso aumenta a transparência do processo e reduz o tempo de busca, por exemplo, de um registro imobiliário. Com essa plataforma a ideia não é substituir os processos existentes, mas sim complementá-los. O objetivo é reforçar o procedimento físico hoje em funcionamento. O serviço garante a autenticidade dos registros da propriedade, o histórico (cadeia dominial) e as transferências. A ferramenta também tem sido utilizada para outros setores além do imobiliário.[12]

A Ubiquity está desenvolvendo um projeto piloto em parceria com o Cartório de Registro de Imóveis no Brasil nos municípios de Pelotas e Morro Redondo, ambas cidades do estado do Rio Grande do Sul, para melhorar o processo de registro de imóveis. O mecanismo de validação pode evitar fraudes e corrupção nos registros. O projeto trouxe mais eficiência e transparência ao processo tradicional.[13]

A empresa Original My oferece uma plataforma de serviços em blockchain que traz mais segurança, credibilidade, agilidade, economia de tempo e custos. A empresa surgiu em 2015 utilizando blockchain para mudar a forma como a autenticidade é tratada no Brasil e no mundo. Através de uma plataforma totalmente automatizada, é possível registrar em blockchain

[11] https://www.ledgerinsights.com/company-formation-blockchain/
[12] https://www.ubitquity.io/. Acesso em: 21/04/2019.
[13] http://ubitquity.io/UBITQUITY-CaseStudy.pdf. Acesso em: 21/04/2019.

e verificar a autenticidade de documentos digitais, contratos e identidade de pessoas, além da possibilidade de assinar documentos através do aplicativo e fazer *login* em sites sem preencher senhas ou formulários de quaisquer tipos.[14]

Em uma parceria com o Cartório Azevêdo Bastos, em João Pessoa, Paraíba, Brasil, a plataforma também oferece uma opção de serviço de registro documental na rede blockchain e autenticação pelo cartório.

Um sistema eletrônico de votação também foi desenvolvido pelo CEO da empresa Original My, Edilson Osorio Junior, que defende que para um sistema de votação ser confiável deve permitir ampla auditoria e verificação. Para atingir um extraordinário nível de transparência, todas as cédulas de votação e os votos devem ser públicos. Como o excesso de transparência compromete o direito de privacidade, o modelo hoje utiliza um boletim privado para o registro, contagem e publicação dos votos. A fim de manter o sigilo da identidade dos eleitores, o processo eletrônico de votação via blockchain requer uma primeira rodada de registro dos votantes para só então, num segundo momento, os eleitores registrarem o seu voto propriamente dito. Isso consome muito tempo e recursos. A solução desenvolvida utiliza "stealth addresses" com "zero-knowledge proof-of-vote", encriptação "Paillier" para os votos, a rede Ethereum como plataforma para o armazenamento público e contratos inteligentes para permitir auditorias ao sistema durante e depois das votações. [15]

Registros hospitalares também são objeto das soluções em redes blockchain. As empresas Hashed Health e MedRec estão registrando prontuários de pacientes em hospitais em redes blockchain. Assim possibilitam o compartilhamento dos dados de forma segura e instantânea. Um médico à distância pode emitir um laudo de um exame ou realizar uma perícia remotamente apenas efetuando um registro na rede, que será validado pelos demais participantes. A unicidade do histórico dos dados também é uma característica desejável para que não reste duvidas, por exemplo, sobre a data de realização de cada exame e de cada consulta.

O registro de propriedade intelectual nas redes blockchain também tem sido estudado por algumas empresas no mundo. Muitas vezes o maior desafio é saber qual dos agentes que reivindicam determinada autoria sobre uma marca foi de fato o precursor. O registro imediato

[14] https://originalmy.com/about#. Acesso em: 21/04/2019.
[15] OSORIO JR., 2018

de uma ideia, de uma marca ou de uma música na rede confere um selo de tempo e autenticidade ao registro que futuramente comprovará o direito da propriedade intelectual daquele bem intangível. Uma empresa sueca, a Mind Ark, pretende desenvolver tecnologia para realizar a troca de ativos de propriedade intelectual. Alega entre as vantagens já mencionadas um potencial de redução dos custos para manutenção da patente.

1.6 IMPLICAÇÕES JURÍDICAS

Diante do enorme potencial de uso das redes blockchain em novas soluções digitais, é preciso entender as implicações jurídicas e a repercussão dessa tecnologia na forma como nos relacionamos. Os atributos inerentes às redes e os riscos associados levantam preocupações para o futuro próximo, tais como que tipo de responsabilidades terão essas plataformas, como farão a prevenção de fraudes, sonegações e outros crimes facilitados pelo anonimato, que valor probatório ou de autenticidade terão os registros efetuados nessas redes, entre outras questões.

O primeiro aspecto a ser discutido é qual o Direito a ser aplicado na responsabilização de soluções e aplicações desenvolvidas em redes blockchain. Em casos como invasão de privacidade e abuso de poder econômico suscetíveis de ocorrerem nessas redes, a responsabilização será de cada nó? Será de toda a rede? Será do usuário?

O Direito deverá pensar em alternativas de aplicar o Direito não apenas aos cidadãos individualmente e sim a uma rede virtual. Como aproveitar conceitos e princípios do direito comercial, civil, penal a esse novo direito cibernético.

Como deve ser a aplicação do Direito para responsabilização de eventuais danos provocados por um serviço executado em uma rede blockchain? Os participantes da rede devem ser responsabilizados solidariamente? Só aqueles que detêm o direito de propriedade do software? Antes de alegar que o Código é o Direito, precisamos definir a base legal dessa rede.

As transações individuais executadas na rede são possivelmente contratos, que trazem consigo todas as consequências jurídicas impostas aos contratos realizados no mundo não virtual. Os contratos estabelecidos nas redes são apenas codificados, registrados e validados de forma virtual, mas não deixam de representar uma relação entre indivíduos. Toda transação é passível de gerar responsabilização em caso de falha, o que, no mundo não virtual, significa

dizer que as obrigações serão exigidas e potencialmente a lei de falências ou o próprio código civil pode ser utilizado para fins de apuração da responsabilidade.

As redes distribuídas têm um arranjo diferente das redes de negócios centralizadas, tais como franquias ou cadeias produtivas, em que há um ente central e diversas entidades com relações bilaterais diretamente conectadas ao centro. Nas redes distribuídas, todos estão no mesmo nível hierárquico e conectados entre si. “É o ponto de inflexão em que a rede é um conjunto de entidades de interesses privados que se transforma em um grupo de entidades legalmente conectadas”.

As redes podem ser compreendidas, segundo explicam os autores (ZETZSCHE, BUCKLEY, ARNER, 2018), como *joint ventures*, um contrato de múltiplas partes ou uma sociedade. Independentemente do modelo associado à rede, haverá responsabilização de todos os nós que constituem a rede e principalmente daqueles que de alguma forma desempenham tarefas de projeto, controle e manutenção.

Embora este trabalho pudesse se aprofundar nas questões de responsabilização ou nas questões de fraude e crimes associados a rede, a ênfase será dada sobre a validade jurídica desses dados inseridos nas redes blockchain. Qualquer registro inserido deverá ser considerado autêntico? Qualquer rede blockchain confere essa publicidade e fé pública aos documentos nela inseridos? Para avançar na elucidação dessas questões, é preciso entender o que são provas documentais para o Direito Brasileiro. Quais as normas pertinentes ao tema que poderão esclarecer se essa nova tecnologia pode ou não ser confiável para o Direito.

2 PROVAS

As provas, na lição de Alexandre Freitas Câmara (CÂMARA, 2019), são todos elementos trazidos ao processo para contribuir com a formação do convencimento do juiz a respeito da veracidade das alegações concernentes aos fatos da causa. Ocorre que ao juiz incumbe estabelecer, ao decidir a causa, quais dessas alegações são ou não verdadeiras e, para isso, é preciso que ele forme seu convencimento. E para que tal convencimento possa formar-se, é preciso que sejam trazidos ao processo elementos que contribuam com sua formação. Pois tais elementos são, precisamente, as provas.

Fala-se da prova como um elemento trazido ao processo (dado objetivo) e se alude a sua capacidade de contribuir para a formação do convencimento (dado subjetivo). A junção desses dois aspectos permite a compreensão do que seja, então, para o processo, a prova.

A prova tem por objeto demonstrar a veracidade de alegações sobre fatos que sejam controvertidas e relevantes. Veja-se, então, que o objeto da prova não é o fato, mas a alegação. Demonstra-se que uma alegação, feita no processo, é verdadeira. Feitas estas ressalvas, porém, o objeto da prova é limitado às alegações sobre fatos. Não é, porém, qualquer alegação sobre fato que integra o objeto da prova. Impende que tal alegação seja relevante e controvertida.

As provas podem ser classificadas em diferentes grupos, tais como diretas e indiretas, materiais e imateriais, entre diversas possibilidades. Neste trabalho, nos interessa a classificação quanto à forma estabelecida por Moacyr Amaral Santos (SANTOS, 1970), que enumera as diferentes maneiras pelas quais as provas podem ser apresentadas em juízo:

a) **orais**: em sentido amplo, é a afirmação pessoal oral. No quadro das provas orais estão as provas testemunhal, depoimento de parte e confissão etc.;

b) **documentais**: afirmação escrita ou gravada, escrituras públicas ou particulares, cartas missivas, plantas, projetos, desenhos, fotografias etc.;

c) **material**: consiste em qualquer materialidade que sirva de prova do fato probando; é a atestação emanada da coisa: o corpo de delito, os exames periciais, os instrumentos do crime etc.

2.1 MEIOS DE PROVA

Meios de prova, conforme ensina Câmara (CÂMARA, 2019), são os mecanismos através dos quais a prova é levada para o processo. Alguns deles estão expressamente previstos em lei (como a prova testemunhal ou a documental, por exemplo) e, por isso, são chamados de provas típicas (ou meios típicos de prova). Além desses, porém, admite-se a produção de meios de prova que não estão previstos expressamente, as chamadas provas atípicas (ou meios atípicos de prova).

O art. 369 do Código de Processo Civil estabelece que as partes "têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz".

Provas Típicas

São meios de prova típicos a prova pericial, a prova documental, a prova testemunhal, o depoimento pessoal, a inspeção judicial, a prova emprestada e a confissão. (DIDIER, 2015)

Típicas: Oral, Documental ou técnica

Assim é que, entre as provas típicas, existem provas *orais, documentais* e *técnicas,* conforme classifica Câmara (CÂMARA, 2019).

Prova oral é a que se produz através de um depoimento falado. Pertencem a essa categoria o depoimento pessoal e a prova testemunhal.

Provas documentais são os registros gravados de fatos. Nesta categoria se encontram a prova documental *stricto sensu* (aqui incluída a prova produzida através de documento eletrônico) e a ata notarial.

Provas técnicas são os meios de prova que são produzidos através da análise que alguém faz de um objeto ou pessoa, valendo-se de seu conhecimento especializado. Nesta categoria se encontram a prova pericial e a inspeção judicial.

Provas Atípicas

Meio atípico de prova (CÂMARA, 2019) é o meio de prova que não está previsto expressamente em lei. Bom exemplo disso é a assim chamada "prova de informações", meio de prova que está expressamente previsto em algumas legislações estrangeiras (como é o caso

dos arts. 190 a 192 do Código uruguaio de 1988 e dos arts. 204 e 205 do Código boliviano de 2013, que preveem a *prueba por informe*), mas não foi tipificado no ordenamento processual brasileiro. A prova de informações é a declaração dada por um órgão ou pessoa jurídica, de direito público ou privado, sobre pontos claramente individualizados que resultem de seus arquivos ou registros. Pense-se, por exemplo, no caso de em um determinado processo ser necessária a produção de prova sobre se determinada pessoa esteve ou não em certa cidade em um dia em que ocorreram eleições e, para a produção da prova, se solicita ao Tribunal Regional Eleitoral que informe se aquela pessoa, naquele dia, votou ou justificou ausência (e, caso o tenha feito, em que cidade estava ao apresentar sua justificativa). Pois a apresentação, pelo TRE, de um dado constante de seus arquivos, constitui uma prova de informações.

São meios de prova atípicos, segundo o entendimento de Didier Jr. (DIDIER JR, 2015), por exemplo, a prova estatística, a prova por amostragem (sobre o tema, ver subitem abaixo, no item sobre presunções judiciais), a prova cibernética e a reconstituição de fatos. São provas atípicas (inominadas), pois, com elas, se busca "a obtenção de conhecimentos sobre fatos por formas diversas daquela prevista na lei para as provas chamadas típicas". E a ausência de disciplina legislativa exige que o juiz atente, no momento da sua produção, para os princípios que norteiam o direito probatório, sobretudo o princípio do contraditório.

Pode-se concluir que outros meios de prova que não foram previstos em lei ainda assim podem ser produzidos, admitindo-se novas modalidades de provas no processo civil, contanto que não sejam ilícitas e sejam moralmente legítimas.

Típica ou atípica, a prova será admitida se for lícita. É que, por força do disposto no art. 5º, LVI, da Constituição da República, “são inadmissíveis, no processo, as provas obtidas por meios ilícitos”. Assim, exemplifica o professor Alexandre Câmara (CÂMARA, 2019), confissões obtidas mediante tortura, correspondência obtida mediante invasão de caixas de correio eletrônico, gravações clandestinas de conversas, entre outras, são inadmissíveis no processo em razão da ilicitude de sua obtenção.

Ata Notarial

Chama-se ata notarial ao documento público lavrado por notário através do qual este declara algo que tenha presenciado, declarando sua existência e modo de ser. É figura que se incorporou ao Direito brasileiro pelo art. 7º, III, da Lei nº 8.935/1994, que estabelece que aos tabeliães de notas compete, com exclusividade, lavrar atas notariais. E este dispositivo se

relaciona diretamente com o art. 6º, III, do mesmo diploma, por força do qual aos notários compete autenticar fatos.

O art. 384 do CPC estabelece que "a existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião".

A ata notarial é um instrumento público de grande relevância no direito probatório. É que através dela é possível a documentação de fatos transeuntes, cuja prova por outros meios pode ser muito difícil.

Os notários são dotados de fé pública, o que implica dizer que suas declarações geram uma presunção relativa (*iuris tantum*) de veracidade do que tenha sido declarado.

Do ponto de vista do direito processual civil, a ata notarial deve ser tratada como um documento público, a ela se aplicando todo o regime da prova documental que incide sobre os documentos públicos em geral, especialmente os arts. 405, 427 e 434 a 437.

A sua elaboração independe de qualquer demonstração, ao tabelião contratado, da utilidade ou finalidade da prova, tampouco a sua utilização num procedimento de solução de litígio depende da investigação do interesse ou da finalidade que moveram a sua elaboração.

Por se tratar de documento público, a ata notarial faz prova não só da sua formação, mas também dos fatos que o tabelião declarar que ocorreram em sua presença (art. 405, CPC). Quando utilizada em juízo, no entanto, é preciso ter em mente que se trata, normalmente, de meio de prova produzido unilateralmente. Por mais que o tabelião goze de fé pública, a documentação normalmente é feita sem a presença da parte contra quem o documento é produzido no processo - que, por isso mesmo, não pode interferir no procedimento probatório, tal como teria o direito (fundamental) de fazer caso a mesma diligência fosse realizada em juízo.

Com isso queremos dizer (DIDIER JR., 2015) que a ata notarial é um excelente meio de documentação de fatos, sobretudo por prescindir da deflagração de um procedimento judicial -- como o da produção antecipada de prova (art. 381 e seguintes, CPC) - para alcançar a finalidade que dela se espera. Isso, contudo, não afasta a necessidade de o juiz dar-lhe o valor que, no caso concreto, ela merece, inclusive repetindo, se for o caso, a diligência outrora efetivada pelo tabelião, a fim de que a parte contra quem foi produzida possa, como lhe é de direito, participar da produção da prova.

2.2 PROVA DOCUMENTAL

Documento, na lição de Câmara (CÂMARA, 2019) é toda atestação, escrita ou por qualquer outro modo gravada, de um fato. Assim, são documentos os escritos, as fotografias, os vídeos, os fonogramas, entre outros suportes capazes de conter a atestação de um fato qualquer.

Prova documental, na visão de Marinoni (MARINONI, ARENHART, MITIDIERO, 2015) é aquela oriunda de todas as coisas que são idôneas à documentação de um fato – narrando-o, representando-o ou reproduzindo-o. Documento é uma coisa que tem em si a virtude de fazer conhecer, sendo resultado de um trabalho humano. Documento é uma coisa que narra, representa ou reproduz de forma idônea alguma coisa por força da atividade humana. O conceito de documento compreende todo objeto suscetível de fazer prova de alguma proposição, quer seja escrito ou não. O que interessa é o significado probante.

Público ou Privado

Documentos podem ser públicos ou privados. São públicos aqueles produzidos por um agente público, como um escrivão, chefe de secretaria ou outro servidor público ou, ainda, por um tabelião. Privados são todos os demais documentos. O documento público feito por oficial público incompetente ou que não observe as formalidades legais, tendo sido subscrito pelas partes, equivale, para efeitos probatórios, a um documento particular (art. 407, do CPC).

> Será público quando o seu autor imediato for agente investido de função pública, e quando a formação do documento se der no exercício desta função [...]. Será, ao contrário, particular o documento quando sua autoria imediata se dê por ação de um particular ou mesmo de um funcionário público (desde que este não se encontre no exercício de suas funções) (MARINONI, ARENHART, MITIDIERO, 2015)

Há presunção legal de autenticidade do documento público, entre as partes e perante terceiros, fato que decorre da atribuição de fé pública conferida aos órgãos estatais. Esses documentos contêm afirmações que se referem: (a) às circunstâncias de formação do ato, como data, local, nome e qualificação das partes etc., e (b) às declarações de vontade, que o oficial ouvir das partes.

Para Theodoro Jr. (THEODORO Jr, 2018), a presunção da veracidade acobertada pela fé pública do oficial só atinge os elementos de formação do ato e a autoria das declarações das

partes, e não o conteúdo destas mesmas declarações. Pela verdade das afirmações feitas perante o oficial, só mesmo os autores delas são os responsáveis.

Instrumento Público

Sempre vale recordar que em alguns casos a lei substancial exige que o ato jurídico seja realizado por instrumento público. São os casos em que essa forma é exigida *ad substantiam*. É o que se dá, por exemplo, no caso da emancipação (art. 5º, parágrafo único, I, do CC), do mandato que confere poderes especiais para casar o mandante (art. 1.542 do CC), além dos atos que tenham por objetivo a constituição, transferência, modificação ou renúncia de direitos reais sobre imóveis de valor superior a trinta vezes o maior salário mínimo vigente no Brasil (art. 108 do CC). Pois nestes casos, a ausência do instrumento público não pode ser suprida por qualquer outro meio de prova (art. 406).

Trata-se de resquício, na compreensão de Marinoni *et al* (MARINONI, ARENHART, 2016) do sistema de tarifamento das provas, ou da prova legal. O legislador atribui, prévia e abstratamente, ao instrumento público um valor probatório exclusivo, colocando-o numa posição hierarquicamente superior à dos demais meios de prova. Com isso, cria uma espécie de ponte entre o direito material e o processual, na medida em que, se o direito material reputa nulo (ou inexistente) o ato jurídico que não se revestiu da forma por ele exigida, esta nulidade (ou inexistência) dar-se-á em todas as esferas, inclusive na esfera processual.

Presunção de veracidade relativa em relação ao signatário

Em um documento particular, as declarações que dele constem, desde que o instrumento esteja assinado (tendo ou não sido escrito por quem assinou), se presumem verdadeiras em relação ao signatário (art. 408). Trata-se, evidentemente, de presunção relativa, *iuris tantum*, que pode ser afastada por prova em contrário. Caso o documento particular contenha apenas a declaração de ciência de um determinado fato, considera-se provada a ciência, mas não o fato em si, cabendo ao interessado o ônus da prova de que o fato realmente ocorreu (art. 408, parágrafo único).

Autenticidade do documento particular

O documento particular se considera autêntico quando a assinatura do seu autor tiver sido reconhecida por tabelião (trata-se do reconhecimento de firma, figura muito conhecida do público em geral), nos termos do art. 411, I. Mesmo sem ter havido o reconhecimento de firma, porém, é possível reputar autêntico o documento particular. Basta que a autoria esteja identificada por qualquer outro meio legal de certificação, inclusive eletrônico (art. 411, II) ou se não houver impugnação de sua autoria pela parte contra quem o documento tenha sido produzido no processo (art. 411, III).

O que se exige para a formação de um documento é a autoria, na visão de Didier (DIDIER Jr, 2015). A subscrição serve para provar a autoria, mas, como se viu, não é a única forma, pois até mesmo os documentos escritos podem ter a sua autoria provada de outras formas, como pelo exame grafológico ou mesmo pela presunção de autenticidade decorrente da admissão expressa ou tácita do documento.

Impressão de e-mails, fotografias digitais, imagens da internet

Fotografias digitais ou extraídas da Internet fazem prova das imagens que reproduzem, devendo – se houver impugnação – ser apresentada a respectiva autenticação eletrônica. Não sendo isto possível, será realizada perícia (art. 422, § 1º). Caso se trate de fotografia publicada em jornal ou revista, será exigido um exemplar original do periódico caso sua veracidade seja impugnada (art. 422, § 2º). Tudo isso é também aplicável à forma impressa de mensagens eletrônicas (como *e-mails*, por exemplo), nos termos do § 3º do art. 422.

Podem as repartições públicas fornecerem toda a documentação requisitada em meio eletrônico, certificando, pelo mesmo meio, que se trata de extrato fiel do que consta em seu banco de dados ou no documento que tenha sido digitalizado (art. 438, § 2º).

2.3 DOCUMENTO ELETRÔNICO

Tradicionalmente, o meio físico clássico que as pessoas normalmente utilizam para a representação de fatos e ideias é o papel. Com a evolução tecnológica, outras espécies conquistaram espaço para dar suporte a documentação escrita desses fatos e ideias. Exemplos disso são os chamados documentos eletrônicos, que têm existência meramente virtual e não estão associados a nenhum meio físico que lhes sirva de suporte. No entanto, para que possam ser apresentados em juízo, na compreensão de Didier Jr. (DIDIER Jr, 2015) muitas vezes

precisam ser acondicionados em dispositivos de armazenamento de dados (p. ex., mídias, pen-drives etc.), salvo se o processo em que será inserido for também virtual (ou processo eletrônico).

Segundo a lição de Augusto Tavares Rosa Marcacini (MARCACINI, 1999), "o documento eletrônico é [...] uma sequência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital".

Têm tratamento específico e diferenciado na lei processual os documentos eletrônicos, especialmente por conta de sua produção naquilo que o art. 439 do CPC, chama de “processo convencional” (mas que, na verdade, é o processo cujos autos não são eletrônicos, sendo impressos em papel) (THEODORO JR, 2018). Pois estabelece o próprio art. 439 que nesses casos o documento produzido eletronicamente só será admitido no processo se for convertido à forma impressa, devendo ser verificada sua autenticidade.

Caso o documento eletrônico não seja convertido à forma impressa, porém, o juiz apreciará seu valor probante, assegurado às partes o acesso ao seu teor (art. 440 do CPC). Serão admitidos como fontes de prova os documentos eletrônicos que tenham sido produzidos e conservados nos termos da legislação específica (art. 441 do CPC).

Como regra geral, os documentos eletrônicos deverão ser produzidos observando-se o disposto na Medida Provisória Nº 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, a qual se destina a assegurar a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (art. 1º da MP Nº 2.200-2/2001).

Além da autenticação por serviço notarial, a autenticidade pode ser presumida em razão de outros meios legais previstos para esse fim. Em especial, importa fazer referência à certificação digital, a que alude, por exemplo, o art. 10 da Medida Provisória nº 2.200-2/2001.

Os documentos eletrônicos podem ser públicos ou particulares (art. 10 da MP nº 2.200-2/2001), sendo certo que os documentos eletrônicos produzidos com a utilização do processo

de certificação da ICP-Brasil se presumem verdadeiros em relação aos seus signatários (art. 10, § 1º, da MP nº 2.200-2/2001 e art. 219 do CC).

Documentos eletrônicos não produzidos com a observância do disposto na Medida Provisória que regulamenta a ICP-Brasil também podem ser admitidos, desde que se utilize algum outro meio de comprovação de autoria e integridade de tais documentos em forma eletrônica, inclusive os que usem certificados não emitidos pela ICP-Brasil, desde que admitidos pelas partes como válidos ou aceitos pela pessoa a quem o documento for oposto (art. 10, § 2º, da MP nº 2.200-2/2001).

Aos documentos eletrônicos, na compreensão de Didier (DIDIER JR, 2015), se aplica, quanto ao mais, toda a regulamentação da prova documental, tanto no que concerne à sua força probante como no que se refere à sua produção. Para que se possa atribuir valor probatório aos documentos eletrônicos, é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua autenticidade, que permite identificar a sua autoria, e à sua integridade, que permite garantir a inalterabilidade do seu conteúdo. Somente a certeza quanto a esses dados é que poderá garantir a eficácia probatória desses documentos[16].

Essa é uma preocupação constante, já que a evolução tecnológica aponta no sentido de que esses documentos serão cada vez mais utilizados, sobretudo no trânsito jurídico de bens e serviços. O problema é que, pelo seu próprio conceito (sequência de bits representativa de um fato), já se vê que a maior e melhor característica do documento eletrônico - que é a sua versatilidade, ou flexibilidade, na medida em que, em segundos, ele pode ser formado e utilizado, mediante envio pela Internet, em qualquer lugar do mundo - é também a porta para possíveis adulterações, o que infirma a sua integridade e, pois, a sua eficácia probatória.

Ademais, o parágrafo 2º do art. 18 da Res. nº 1/2010 da Presidência do STJ preconiza que "o envio da petição por meio eletrônico e com assinatura digital dispensa a apresentação posterior dos originais ou de fotocópias autenticadas". É mais uma ratificação no âmbito do Tribunal de que a autenticação dos documentos eletrônicos é suficiente para a validade dos mesmos perante a justiça.

[16] O enunciado nº 297 das jornadas de Direito Civil do Conselho da Justiça Federal: "O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada".

Criptografia Simétrica e Assimétrica

Associado diretamente à integridade e autenticidade das assinaturas digitais estão os métodos e algoritmos de criptografia. Para tanto, vale diferenciar duas formas básicas de criptografia: simétrica e assimétrica, sendo a última a que mais nos interessa nesse estudo em razão de ser utilizada pelas redes blockchain.

Como ensina Antônio Lago Jr. (LAGO JR., 2001), "o uso da criptografia simétrica, também chamada de criptografia de chave privada, requer que o destinatário da mensagem conheça o algoritmo usado para cifrar o seu conteúdo, caso contrário, ficará impossibilitado de decifrar a mensagem, ou seja, o destinatário da mensagem deve ter acesso à chave utilizada pelo remetente". Esse método é frágil em termos de segurança, na medida em que a chave utilizada para decifrar a mensagem é a mesma utilizada para cifrá-la. Assim, sendo ela conhecida pelo receptor, não se pode garantir que ele não venha utilizá-la para cifrar novas mensagens, fazendo-se passar pelo autor da mensagem originária. Isso infirmaria, como se pode ver, talvez não a autenticidade da mensagem recebida, mas de tantas outras que, a partir da chave conhecida, pudessem vir a ser formadas.

Já a criptografia assimétrica é uma das técnicas capazes de conferir maior segurança quanto à autenticidade e integridade do conteúdo do documento eletrônico. Explica-nos Augusto Marcacini (MARCACINI, 1999): "A criptografia assimétrica, ao contrário da convencional (que pede a mesma chave tanto para cifrar como para decifrar a mensagem), utiliza duas chaves, geradas pelo computador. Uma das chaves dizemos ser a chave privada, a ser mantida em sigilo pelo usuário, em seu exclusivo poder, e a outra, a chave pública, que, como sugere o nome, pode e deve ser livremente distribuída. Estas duas chaves são dois números que se relacionam de tal modo que uma desfaz o que a outra faz. Encriptando a mensagem com a chave pública, geramos uma mensagem cifrada que não pode ser decifrada com a própria chave pública que a gerou. Só com o uso da chave privada poderemos decifrar a mensagem que foi codificada com a chave pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada, só poderá ser decriptado com a chave pública."

A chave privada, utilizada por aquele que formou o documento eletrônico, gera uma assinatura digital, que permite a identificação do seu autor. Essa assinatura digital pode ser conferida a partir do uso da chave pública. Não se trata, contudo, de um sinal visível, como o é a assinatura manuscrita, mas de uma sequência numérica a que o programa de computador

chega a partir de fórmulas matemáticas. A assinatura digital será diferente para cada documento gerado por uma determinada chave privada, mas sempre estará vinculado a ela, o que garante a prova da autenticidade do documento.

Além de essa chave privada poder atestar a autenticidade do documento, ela ficará vinculada ao seu conteúdo, de modo que qualquer alteração superveniente tornará, automaticamente, ineficaz a assinatura digital outrora lançada. Com isso, embora seja possível a alteração do conteúdo do documento guardado pela criptografia assimétrica, essa alteração não mais vinculará o seu autor originário. Em outras palavras: a integridade do documento é garantida em relação ao seu autor; não sendo possível identificá-lo, tem-se aí um indício de que o documento foi alterado.

Como se viu, somente a chave pública distribuída por uma determinada pessoa pode ser utilizada para decifrar a mensagem codificada pelo titular da respectiva chave privada. Mas aí surge um novo problema (MARCACINI, 1999): "qualquer um poderia gerar um par de chaves e atribuir-lhe o nome de qualquer pessoa, existente ou imaginária. A autenticidade do documento eletrônico é conferida sem dificuldade por qualquer usuário de computador, com o uso do programa de criptografia e de posse da chave pública do seu subscritor. Mas, e se a própria chave pública não for autêntica? Esta conferência o programa não tem como realizar. O que fazer, então, para contornar o problema?". Nesse caso, a assinatura digital apontaria, como autor do documento, uma determinada pessoa, distinta da que efetivamente formara o documento.

Como ensina Antônio Terêncio G. L. Marques (MARQUES, 2005), "para evitar, então, essa fraude, instituiu-se a certificação digital, onde a identidade do proprietário das chaves é previamente verificada por uma terceira entidade de confiança dos interlocutores, que terá a incumbência de certificar a ligação entre a chave pública e a pessoa que a emitiu, como também a sua validade". Essa terceira entidade a que alude o autor, responsável pela certificação digital da identidade do proprietário das chaves e pela divulgação ao público das chaves públicas válidas, é a chamada autoridade certificadora.

3 VALIDADE JURÍDICA DAS PROVAS EM BLOCKCHAIN

Em consonância com o disposto no Código Civil, em seu art. 212, se um determinado negócio não impor uma forma especial de comprovação, o fato jurídico pode ser provado mediante documento, entre outras formas.

O Marco Civil da Internet, Lei nº 12.965/2014, estabelece em seu art. 22 que "a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet".

A própria lei prevê hipótese em que o juiz ordenará a guarda dos registros de conexão ou de acessos a aplicações na internet para fazer prova em processos judiciais cíveis ou penais. É o caso, por exemplo, de o juízo determinar que o *Facebook* mantenha os registros de acesso de um determinado usuário em sua rede para eventual comprovação de um crime ou ato ilícito praticado na rede social.

Embora o Marco Civil da internet seja uma legislação recente e que trata, entre outras questões, da forma de responsabilização de usuários e provedores de aplicações digitais, algumas questões ficam em aberto. A quem o juiz irá atribuir a responsabilidade de guarda desses registros em soluções que não encontram um ente central responsável pela aplicação? Embora esse ente não exista e não possa ser responsabilizado, a rede apresenta atributos que já foram explorados, tais como a imutabilidade dos registros e a transparência, que garantem que uma vez inseridos na rede lá permanecerão.

Diante dessa compreensão, e interpretando o disposto na Lei, os registros efetuados em uma rede blockchain podem formar um conjunto probatório em processos cíveis ou penais. Podem comprovar, por exemplo, que um determinado acesso ocorreu em uma data e hora específicos. Ou ainda, um fato público e notório pode ser comprovado por meio de registro realizado na rede.

Em concordância com o Código Civil, o CPC também estabelece em seu art. 369 que "as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz".

Uma interpretação mais ampla permite inferir que o art. 441, que admite "documentos eletrônicos produzidos e conservados com a observância da legislação específica", é suficiente para autorizar esses registros em redes blockchain como meio de prova (documento eletrônico) legítimo.

Alexandre Freitas Câmara (CÂMARA, 2019) traz um exemplo em "que se queira provar qual o conteúdo de determinada página na Internet, para o fim de posteriormente postular-se reparação de danos por violação de direitos autorais. É sabido que o conteúdo de páginas eletrônicas da rede mundial de computadores pode ser facilmente alterado e, por isso, nem sempre é fácil produzir prova do que elas contêm. Pois basta pedir a um notário que acesse a aludida página e descreva seu conteúdo."

O autor faz alusão ao recurso da ata notarial, que vem sendo cada vez mais utilizada para comprovação de fatos e acontecimentos nas redes sociais. O instrumento tem previsão legal no art. 384 do Novo CPC, em que "A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião".

3.1 Serventias Extrajudiciais

As serventias extrajudiciais, através de seus tabeliães ou registradores, dão fé pública aos atos por eles praticados. A Lei nº 8.935/94 definiu em seu art. 3º que "notário, ou tabelião, e oficial de registro, ou registrador, são profissionais do direito, dotados de **fé pública**, a quem é delegado o exercício da atividade notarial e de registro." Assim, não há que se questionar a competência delegada do Estado aos registradores para exercerem suas atividades.

A Lei dos Cartórios, Lei nº 8.935/94, estabelece competências aos notários e tabeliães. Aos notários, por exemplo, compete formalizar juridicamente a vontade das partes ou conferir autenticidade a atos e negócios jurídicos (art. 6º). Aos tabeliães compete com exclusividade, entre outras, o reconhecimento de firmas e a autenticação de cópias (art. 7º).

Merece destaque a competência exclusiva desses delegatários do poder público em lavrar escrituras e procurações públicas e testamentos. O registro de imóveis, por exemplo, ou atos de averbação ou retificação na matrícula, são atividades exercidas exclusivamente pelos registradores públicos. Notamos aqui um impedimento legal de outras formas válidas de registro de imóveis. Embora uma aplicação desenvolvida em blockchain possa efetuar esses

registros imobiliários em busca transparência e publicidade, para efeitos perante a justiça, o único registro que comprova a propriedade do imóvel será aquele realizado em cartório de registros.

O art. 9º da Lei ainda dispõe sobre a limitação de atuação territorial do tabelião, que fica impedido de praticar atos foram do Município para o qual recebeu a delegação. Entre algumas aplicações práticas, temos a dificuldade de respeitar essa regra se os registros fossem feitos em redes blockchain que não têm limitações territoriais.

Diante das limitações legais e competências exclusivas dos notários e tabeliães, precisamos primeiro entender que qualquer iniciativa em rede blockchain com o intuito de conferir autenticidade a documentos ou publicidade de fatos, serão iniciativas privadas, sem o mesmo caráter público das serventias. Enquanto a ata notarial, por exemplo, é um documento público, o registro efetuado na rede blockchain pode ser considerado um documento particular.

A ordem cronológica de inserção dos registros também traz grandes repercussões ao direito real. Se dois registros são feitos na mesma matrícula de um imóvel, conferindo a titularidade a duas pessoas distintas, então aquele que primeiro constar da matrícula será de fato o proprietário e o segundo deverá ser indeferido. Esse problema surge quando as redes enfrentam um grande volume de transações, mas não conseguem efetuá-las em tempo hábil. Com isso, há um represamento de transações, que ficam em fila a espera de um novo bloco disponível. Se nessa etapa a última transação for inserida em um bloco anteriormente à primeira transação, então os registros farão prova de uma propriedade erroneamente.

Há necessidade de uma progressão ascendente nas numerações dos livros, mais precisamente de acordo com o art. 7º da lei nº 6.015/73, “os números de ordem dos registros não serão interrompidos no fim de cada livro, mas continuarão, indefinidamente, nos seguintes da mesma espécie”. Portanto, a rede blockchain utilizada em eventual aplicação de registros cartorários deverá ter mecanismo que garanta a ordem cronológica das transações independentemente da lentidão para validação de novos blocos ou de transações órfãs, sob pena de uma violação à lei.

Além das questões objetivas, deve-se frisar que o registrador de imóveis desempenha um papel fundamental na garantia dos dados e informações que serão inseridos na matrícula do imóvel. Em uma escritura de compra e venda, por exemplo, é ele quem verifica a legitimidade das partes na transação, identifica alguma restrição, como, por exemplo, a ausência da autorização uxória e, diante de qualquer inconsistência, comunica o interessado sobre a exigência para cumprimento desta, sob pena de não fazer o registro.

Não obstante a competência dos registradores seja exclusiva para efetuar os registros imobiliários no Brasil, a tecnologia pode auxiliar a prestação desse serviço, proporcionando um ambiente mais integrado, mais ágil e com menor possibilidade de fraude. A tecnologia blockchain tem grande potencial de uso no processo de integração das mais de 5.000 serventias espalhadas país afora.

A possibilidade de realizar a escritura em meio eletrônico é um avanço em relação a um movimento de atualização tecnológica que se iniciou em 2009 com a edição da Lei 11.977. O diploma legal determinou a instituição de Sistema de registro eletrônico e determinou a inclusão nesse Sistema de todos os registros efetuados desde 1973 em prazo máximo de 5 anos. O art. 41, alterado pela Lei nº 13.097/2015 acrescentou que "a partir da implementação do sistema de registro eletrônico de que trata o art. 37, os serviços de registros públicos disponibilizarão ao Poder Judiciário e ao Poder Executivo Federal, por meio eletrônico e sem ônus, o acesso às informações constantes de seus bancos de dados, conforme regulamento".

O referido Sistema foi instituído pela Corregedoria Nacional de Justiça (CNJ), por meio do Provimento nº 47/2015, trata-se do Sistema de Registro Eletrônico de Imóveis (SREI). A ferramenta tem como objetivo facilitar o intercâmbio de informações entre os ofícios de registro de imóveis, o Poder Judiciário, a administração pública e o público em geral. O Sistema permite o acesso do público em geral a serviços de emissão de certidões de imóveis on-line, pesquisa de bens por CPF ou CNPJ, entre outros serviços.

O Sistema deve ser implantado e integrado por todos os oficiais de registro de imóveis de cada estado e do Distrito Federal. O intercâmbio de documentos e informações está a cargo de centrais de serviços eletrônicos compartilhados em cada uma das unidades da federação.[17]

Trata-se de um sistema complexo de registro de imóveis em que atuam diversos atores: os cartórios, espalhados em todo território brasileiro; as prefeituras, que mantêm cadastros para fins de arrecadação do IPTU; a União, com competência de arrecadação do ITR e de regularização fundiária; os proprietários; os membros do Judiciário, que eventualmente terão de penhorar um bem em um processo de execução; entre outros que participam desse sistema, seja alimentando com novas informações, seja apenas consultando um registro.

De maneira análoga, o Sistema Nacional de Gestão de Informações Territoriais (SINTER), instituído pelo Decreto nº 8.764/2016, busca centralizar, em uma base de dados

[17] http://www.cnj.jus.br/sistemas/srei. Acesso em: 13/05/2019.

única, dados geoespaciais e outras informações acerca do registro de terras e imóveis no país, estando altamente correlacionado ao georreferenciamento de imóveis urbanos.

O sistema será administrado pela Receita Federal do Brasil, assessorada pelos registradores e órgãos federais, e receberá dos Sistemas de Registros Eletrônicos dos cartórios brasileiros as informações relativas à titularidade dos imóveis, como as operações de alienações, doações e garantias de posse, auxiliando no processo de gestão e tomada de decisão referente à regularização fundiária.

Os grandes desafios para unificação das bases de dados registrais são: ausência de um número único que represente cada imóvel, sem repetição em nenhum outro ente da federação, e existência de arquivos em meio físico de registros de imóveis em regiões que não tiveram os serviços informatizados.

Superados esses desafios, uma rede blockchain poderia ser implementada para integrar os dados de todos os cartórios no Brasil. Cada participante nessa rede seria um servidor, com uma cópia completa de todos os registros desse imenso banco de dados. Alternativamente, poderia haver apenas um participante nessa rede com características de servidor, com o papel de armazenar uma cópia desse banco de dados. Os demais participantes poderiam participar validando as transações e realizando novos registros, além da possbilidade de consultas.

Uma forma de avanço desse sistema seria possivelmente pela incorporação da tecnologia blockchain aos referidos sistemas. Se uma rede aberta já existente, tal como Bitcoin ou Ethereum, seria a melhor estratégia, caberia aos responsáveis uma análise mais aprofundada. Uma alternativa é a criação de uma rede permissionada em que os "mineradores", aqueles responsáveis pela validação das transações, seriam previamente admitidos pelos órgãos governamentais.

O projeto Notary Ledgers[18], desenvolvido pela empresa Growth Tech[19] em parceria com IBM, Cyrela e alguns cartórios do Rio de Janeiro, efetuou em 28/05/2019[20] o primeiro registro de imóveis no Brasil utilizando a tecnologia blockchain. O projeto foi desenvolvido sobre a plataforma Hyperledger Fabric, rede blockchain desenvolvida em parceria da Linux com a IBM. A rede tem sido utilizada comercialmente por diversas empresas que estão preocupadas com a questão da segurança dessas redes. Alguns especialistas defendem, inclusive, que, sendo

[18] https://www.notaryledgers.com/. Acesso em: 29/05/2019.
[19] https://growthtech.com.br. Acesso em: 29/05/2019.
[20] https://www.facebook.com/1489841374412040/posts/2358724534190382/. Acesso em: 29/05/2019.

uma rede permissionada, em que há um ente responsável, no mínimo, pelo credenciamento inicial dos participantes, então não seria uma rede blockchain propriamente dita e sim uma outra espécie de rede. No entanto, a solução tem sido amplamente utilizada e serviu de ferramenta para o desenvolvimento do Notary Ledgers.

Importante destacar que a operação foi validada pelos cartórios, que não abriram mão de suas competências de registro. Acontece que todo o trâmite é digital. O interessado em efetuar o registro acessa o site do Notary Ledgers e lá cria uma identidade virtual, a partir de seus documentos digitalizados e de sua imagem facial capturada. A partir dessa assinatura digital, o usuário escolhe o serviço, tal como certidão de casamento, certidão de nascimento, registro de imóveis, entre outros. O documento é confeccionado com base nas informações do usuário e enviado para o cartório competente por aquela jurisdição. Ele valida digitalmente o documento, que é devolvido com o mesmo valor legal de um documento físico emitido no cartório. O registro é feito em seguida em uma rede blockchain desenvolvida para o sistema.

Para Cláudio Lóssio (LÓSSIO, 2017), "a vantagem excepcional da utilização da tecnologia *blockchain* dentro das serventias extrajudiciais, é fazer com que os registros de bancos de dados não sejam alterados, excluídos, ou simplesmente não fujam de ordem alguma, assim gerando um maior poder de correição estatal dentro dos cartórios, como também promover a segurança das informações digitais deste, e consequentemente a segurança das informações perante as pessoas que têm seus cadastros junto a esta serventia extrajudicial".

O pesquisador acredita que a tecnologia poderá contribuir para a promoção da segurança, em razão do backup dos dados descentralizado; da proteção do conteúdo, que estará criptografado e acessível apenas às partes que detêm a chave privada, e da união de uma fé pública a uma fé digital.

3.2 Autenticidade, Assinatura Digital e Criptografia

A fim de investigar se os registros nas redes blockchain possuem o mesmo valor probante de documentos públicos, precisamos comprovar a autenticidade de autoria desses registros.

Para os efeitos cíveis, o CPC considera autêntico o documento quando “a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei” (art. 411, II, CPC). Preocupou-se o legislador com a autoria do documento. Não por acaso a ICP Brasil tornou-se a responsável pelo credenciamento de empresas para a emissão de certificados digitais, que conferem autenticidade a esses documentos.

A solução, então, para garantir autenticidade dos registros em blockchain estaria relacionada a certificação prévia de usuários que pudessem obter uma assinatura digital certificada capaz de comprovar a autoria do documento? Embora a rede Bitcoin, por exemplo, seja uma rede que dispensa o uso de credenciamento prévio e é pública, outras camadas de serviço associadas a essa rede, ou outros tipos de rede blockchain, podem atrelar a suas funcionalidades essa certificação exigida pela lei.

Para Marcacini (MARCACINI, 1999) “a segurança jurídica da comunicação, aqui entendida como uma certeza que possa ser demonstrável a um terceiro, só pode ser obtida com o uso de assinaturas geradas pela criptografia de chave pública, eis que este é o único método que impede a alteração unilateral do documento ou registro eletrônico e permite atribuir-lhe autenticidade. A um registro que seja tecnicamente possível, a uma parte, alterar, não se pode atribuir valor probante em face da outra parte, pois isto seria dar azo à autoprodução de prova”.

Embora a rede Bitcoin e outras redes blockchain utilizem-se da combinação de uma chave pública com uma chave privada para os seus usuários, os registros inseridos são imutáveis em razão do encadeamento dos blocos e do mecanismo de validação baseado no PoW. Cada usuário é detentor de uma chave privada que garante o anonimato dos usuários na rede.

O professor estabelece, ainda, duas condições de validade ao documento eletrônico: i) somente a assinatura criptográfica permite que um documento eletrônico seja insuscetível de alteração; ii) documentos eletrônicos não assinados não permitem, por si, que seja demonstrada a sua autoria e, consequentemente, não podem ser propriamente considerados como documentos, enquanto meios de prova.

Sem a possibilidade de identificação de autoria, o documento se assemelha a um contrato verbal, “o registro, em poder de uma parte, e sem a inalterabilidade conferida pela assinatura criptográfica da outra parte, é amplamente suscetível a modificações. Além disso, não se tem a menor certeza acerca da identidade da pessoa com quem se contratou. Não se quer dizer com isso que tais contratos não existam, que sejam inválidos, nem que não possam ser provados. O que temos em mãos, porém, é um contrato cuja forma se assemelha à forma verbal”. (MARCACINI, 1999)

O problema, portanto, estaria na impossibilidade de identificação da autoria do registro. O que confere menor capacidade probatória ao registro, mantendo uma equivalência aos outros meios de prova que não documentos.

Um documento eletrônico assinado digitalmente possui validade de título executivo extrajudicial, segundo o entendimento firmado pela Terceira Turma do STJ em sede do RESP 1.495.920-DF. A preocupação do tribunal concentra-se na autenticidade da assinatura digital e na segurança do contrato eletrônico, ou aquilo que podemos considerar integridade do meio. É o que se depreende do informativo nº 0627, publicado em 29 de junho de 2018:

> De início, registre-se que o rol de títulos executivos extrajudiciais, previsto na legislação federal em numerus clausus, deve ser interpretado restritivamente, em conformidade com a jurisprudência desta Corte Superior. É possível, no entanto, o excepcional reconhecimento da executividade de determinados títulos (contratos eletrônicos) quando atendidos especiais requisitos, em face da nova realidade comercial com o intenso intercâmbio de bens e serviços em sede virtual, visto que nem o Código Civil, nem o Código de Processo Civil, inclusive o de 2015, mostraram-se permeáveis à realidade negocial vigente e, especialmente, à revolução tecnológica que tem sido vivida no que toca aos modernos meios de celebração de negócios, que deixaram de se servir unicamente do papel, passando a se consubstanciar em meio eletrônico. Nesse sentido, **a assinatura digital de contrato eletrônico tem a vocação de certificar**, através de terceiro desinteressado (autoridade certificadora), que determinado usuário de certa assinatura a utilizara e, assim, está efetivamente a firmar o documento eletrônico e a garantir serem os mesmos os dados do documento assinado que estão a ser sigilosamente enviados. Ademais, é necessário destacar que, com base nos precedentes desta Corte, em regra, exigem-se duas testemunhas em documento físico privado para que seja considerado executivo, mas excepcionalmente, poderá ele dar azo a um processo de execução, sem que se tenha cumprido esse requisito formal entendimento este deve-se aplicar aos contratos eletrônicos, desde que observadas as garantias mínimas acerca de sua **autenticidade e segurança**. (REsp 1.495.920-DF, Rel. Min. Paulo de Tarso Sanseverino, por maioria, julgado em 15/05/2018, DJe 07/06/2018)[21]

A encriptação de dados, hashing, assinaturas digitais e a chave pública da rede blockchain possibilitam a comunicação e a circulação de mensagens em uma rede pública sem que os usuários possam ver exatamente o conteúdo de cada mensagem. O blockchain utiliza o mecanismo de duas chaves, uma pública e uma privada. A primeira é utilizada para criptografar a mensagem que será transmitida e a segunda é a que fará a decodificação do conteúdo para o usuário destinatário da mensagem.

[21] REsp 1.495.920-DF, Rel. Min. Paulo de Tarso Sanseverino, por maioria, julgado em 15/05/2018, DJe 07/06/2018.

A assinatura digital é uma forma de encriptação por chave pública. Segundo Tauber (TAUBER, 2018), por meio dela é possível: i) autenticar a identidade do usuário, ii) auferir integridade do conteúdo, iii) e comprovar a autoria.

> A assinatura digital é outra aplicação de criptografia de chave pública, ao assinar o conteúdo da mensagem com um esquema de assinatura digital você pode conseguir três atributos importantes: 1) autenticação da identidade do remetente, 2) integridade do conteúdo da mensagem (mesmo como em qualquer esquema de criptografia de chave pública) e 3) não-repúdio - isto é, o assinante da mensagem não pode se retratar ou negar o fato de que ele é quem assinou e enviou a mensagem em um determinado momento. (TAUBER, 2018)

As funções Hash são algoritmos de encriptação unidirecionais, ou seja, a partir de uma entrada x, obtém-se uma saída y. No entanto, não é possível inferir o conteúdo x a partir de y e da função. Isso garante que, uma vez codificada a informação, só poderá ser decodificada a partir da chave privada. A função Hash é, no caso em tela, o que gera a chave pública. A função Hash utilizada pela rede Bitcoin é a Hash 256, que faz menção à quantidade de bits contidos em cada sequência binária de 64 caracteres.

A integridade dos dados, portanto, é garantida pela criptografia Hash e pela assinatura digital. Uma vez efetuado o registro e dada a imutabilidade dos blocos, teremos a integridade garantida. Assim, é possível autenticar o destinatário de uma mensagem, bem como o momento de recebimento.

> Depois de criptografados, assinados e gravados no blockchain, também podemos comprovar a integridade dos dados, certificando-nos de que eles sejam à prova de falsificação e imutáveis. Podemos até mesmo autenticar um destinatário de uma mensagem de email e validar a hora do recebimento. Os casos de uso no mundo da evidência e da evidência digital são infinitos. Os mais proeminentes estão usando o blockchain como um serviço notarial. Alguns exemplos notáveis são: silentnotery, blocknotery and stamp.io. (TAUBER, 2018)

Partindo do pressuposto de que uma determinada rede blockchain garante a integridade do conteúdo nela registrado e a autenticidade da autoria dos registros, então poderiam enquadrar-se no conceito de documento eletrônico estabelecido pelo enunciado nº 297 da IV Jornada de Direito Civil (CJF/STJ). Admitir-se-ia, portanto, o valor probante desses registros se atendidos os pressupostos de integridade e autoria.

> O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada (Enunciado nº 297 da IV Jornada de Direito Civil)

Nessa lógica, o regime jurídico da prova documental deve ser aplicado aos registros blockchain, tal como são aplicados aos documentos eletrônicos, como estabelece o enunciado nº 298 da IV Jornada de Direito Civil, em que “os arquivos eletrônicos incluem-se no conceito de 'reproduções eletrônicas de fatos e coisa', do art. 225 do Código Civil, aos quais deve ser aplicado o regime jurídico da prova documental".

Recentemente, a MP nº 881/2019, publicada no dia 30/04/2019, trouxe regras e diretrizes com o intuito de desburocratizar a atividade empresarial no país. Trata-se da MP da “Liberdade Econômica”, pois estabelece princípios de facilitação à vida do pequeno empreendedor, a exemplo da possibilidade de funcionarem em qualquer horário e exercerem as atividades que não envolvem riscos sem autorização prévia.

No bojo dessa medida, um dos pilares é a redução do papel na burocracia Brasileira. A proposta, já em vigência, possibilita o armazenamento de documentos em meio digital sem a necessidade de manter os originais em meio físico e confere aos documentos digitais o mesmo valor legal para fins probatórios de uma relação jurídica. O art. 3º enuncia que:

> Art. 3º São direitos de toda pessoa, natural ou jurídica, essenciais para o desenvolvimento e o crescimento econômicos do País, observado o disposto no parágrafo único do art. 170 da Constituição:
>
> .....
>
> X - arquivar qualquer documento por meio de microfilme ou **por meio digital**, conforme técnica e requisitos estabelecidos em regulamento, **hipótese em que se equiparará a documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público**.

As alterações normativas produzem efeitos na interpretação de direito civil, empresarial, econômico, urbanístico, trabalho, consumo, proteção ao meio ambiente, direito tributário e direito financeiro.

A regra é apenas uma formalização da compreensão vigente a respeito da validade dos documentos digitais no ordenamento jurídico brasileiro. Vem ratificar um entendimento adequado à evolução tecnológica, que viabilizou uma série de conquistas, tais como métodos de criptografia muito seguros, maior acessibilidade da população à internet, mecanismos de integridade, validação e transferência de dados, que criaram um contexto de confiança nas informações em meio digital.

A medida vai além, garantindo o mesmo valor probatório do documento original ao documento digital e o mesmo efeito jurídico conferido aos **documentos microfilmados, além de** incentivar o descarte dos originais em meio físico. O art. 11 da medida provisória altera o art. 2º-A da Lei nº 12.682/2012, e estabelece que:

> § 1º Após a digitalização, **constatada a integridade do documento digital nos termos estabelecidos no regulamento**, o original poderá ser destruído, ressalvados os documentos de valor histórico, cuja preservação observará o disposto na legislação específica.
>
> § 2º O documento digital e a sua reprodução, em qualquer meio, realizada de acordo com o disposto nesta Lei e na legislação específica, terão o **mesmo valor probatório do documento original, para todos os fins de direito**, inclusive para atender ao poder fiscalizatório do Estado.
>
> .....
>
> § 4º Os documentos digitalizados nos termos do disposto neste artigo terão o mesmo efeito jurídico conferido aos **documentos microfilmados**, nos termos do disposto na Lei nº 5.433, de 8 de maio de 1968, e regulamentação posterior.

A edição da referida Medida Provisória evidencia a intenção do legislador em conferir maior credibilidade a documentos eletrônicos e novas formas de armazenamento. É uma adequação natural da lei às transformações tecnológicas. Foi como outras alterações ocorreram, tais como a admissão do Correio Eletrônico como prova em processos judiciais ou o aceite dos *prints* de tela pelos tribunais.

3.3 Correio Eletrônico

O correio eletrônico, mais conhecido como *e-mail*, já foi objeto de controvérsia nos tribunais, sobre a possibilidade de fazer prova em processos judiciais sobre fatos alegados ou contratos firmados por meio da troca de mensagens eletrônicas.

A Lei nº 11.419/2006 estabelece que "Fazem a mesma prova que os originais os extratos digitais de bancos de dados, públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem" (art. 365, V).

O STJ, em sede do REsp 1381603, se manifestou em 2016 sobre a possibilidade de utilizar o correio eletrônico na fundamentação de uma ação monitória. No caso em questão, o e-mail foi considerado válido e suficiente para a comprovação do negócio realizado, da existência da dívida, da confissão da devedora e do valor total da dívida. O relator, Ministro

Luis Felipe Salomão, destacou que "a legislação brasileira não proíbe provas oriundas de meio eletrônico e que há mecanismos capazes de garantir a segurança e a confiabilidade dessa correspondência".

> RECURSO ESPECIAL. AÇÃO MONITÓRIA. PROVA ESCRITA. JUÍZO DE PROBABILIDADE. CORRESPONDÊNCIA ELETRÔNICA. E-MAIL. DOCUMENTO HÁBIL A COMPROVAR A RELAÇÃO CONTRATUAL E A EXISTÊNCIA DE DÍVIDA. 1. A prova hábil a instruir a ação monitória, isto é, apta a ensejar a determinação da expedição do mandado monitório - a que alude os artigos 1.102-A do CPC/1.973 e 700 do CPC/2.015 -, precisa demonstrar a existência da obrigação, devendo o documento ser escrito e suficiente para, efetivamente, influir na convicção do magistrado acerca do direito alegado, não sendo necessário prova robusta, estreme de dúvida, mas sim documento idôneo que permita juízo de probabilidade do direito afirmado pelo autor.
>
> 2. O correio eletrônico (e-mail) pode fundamentar a pretensão monitória, desde que o juízo se convença da verossimilhança das alegações e da idoneidade das declarações, possibilitando ao réu impugnar-lhe pela via processual adequada.
>
> 3. O exame sobre a validade, ou não, da correspondência eletrônica (e-mail) deverá ser aferida no caso concreto, juntamente com os demais elementos de prova trazidos pela parte autora.
>
> 4. Recurso especial não provido.
>
> (REsp 1381603 MS 2013/0057876-1. Relator: Ministro Luis Felipe Salomão. DJ: 11/11/2016).[22]

Merece destaque a preocupação dos magistrados a respeito da autenticidade das mensagens, da confidencialidade e integridade de seu conteúdo, e da irrefutabilidade de autoria como dimensões necessárias para que o documento eletrônico tenha valor probatório.

O relator, Ministro Luis Felipe Salomão, também se manifestou quanto à força probante do documento eletrônico, ressaltando que "o maior questionamento está adstrito ao campo da veracidade e da autenticidade das informações, principalmente sobre a propriedade de determinado endereço de e-mail. Em outras palavras, consiste em saber se uma 'conta de e-mail' pertence às partes da demanda monitória, bem como se o seu conteúdo não foi alterado durante o tráfego das informações."

Na mesma decisão, a Turma reconhece que "há mecanismos capazes de garantir a segurança e a confiabilidade da correspondência eletrônica e a identidade do emissor, permitindo a trocas de mensagens criptografadas entre os usuários. É o caso do e-mail assinado digitalmente, com o uso de certificação digital."

Por fim, deve-se mencionar que a possibilidade de impugnação de autenticidade de documentos não está adstrita a documentos eletrônicos. Ao contrário, a tecnologia e os

[22]https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1545173&num_registro=201300578761&data=20161111&formato=PDF. Acesso em: 29/05/2019.

mecanismos de segurança e criptografia garantem crescente confiabilidade e mitigação de fraudes de autenticidade.

Na esteira das decisões do STJ, pode-se traçar uma analogia entre as mensagens eletrônicas de e-mails e os registros eletrônicos em blockchain. Embora sejam objetos digitais distintos, ambos estão dotados da possibilidade de transportar e tornar público algum fato ou informação relevante para a comprovação de um ato ou negócio jurídico. A maior preocupação, portanto, estaria em aferir se os registros nas redes blockchain são autênticos, íntegros e irrefutáveis. Quanto a confidencialidade, não deve ser um requisito, tendo em vista que o fato pode ser público e o registro por sua vez também dará publicidade a informação.

Assim, parece que a integridade é inerente à própria arquitetura das redes blockchain, que garantem a imutabilidade dos registros, em regra. Quanto a autenticidade e irrefutabilidade, são critérios que, a depender da rede, podem ser garantidos. A rede Bitcoin, por exemplo, não oferece esse mecanismo de autenticidade dos registros, tendo em vista que respeita o anonimato dos usuários. Em decorrência, difícil seria comprovar que um determinado registro ou informação refere-se a uma pessoa A ou B. Outras redes permissionadas são capazes de garantir essas características.

3.4 Print de Tela

O Supremo Tribunal Federal já resvalou a questão quando analisou a Queixa-Crime proposta pelo Senador Romero Jucá contra o também Senador Telmário Mota, nos autos da Ação Originária – AO 2002/DF, aceitando até mesmo imagem da tela (*prints*) do aparelho móvel a representar mensagens trocadas pelo WhatsApp como prova dos fatos discutidos na demanda.

> Queixa-crime. Ação penal privada. Competência originária. Crimes contra a honra. Calúnia. Injúria. Difamação. 2. Justa causa. Prova das declarações. Inexistência de gravação das entrevistas e de ata notarial quanto a ofensas por redes sociais. As declarações ofensivas à honra podem ser provadas por qualquer meio, sendo desnecessária a vinda aos autos de gravação original ou de ata notarial. A petição inicial é instruída com a transcrição das entrevistas e com o registro das declarações alegadamente veiculadas por redes sociais. A documentação produzida é suficiente para, na fase processual atual, demonstrar a existência do fato. 3. Art. 53 da Constituição Federal. Imunidade parlamentar. Ofensas em entrevistas a meios de comunicação de massa e em postagens na rede social WhatsApp. O manto protetor da imunidade alcança quaisquer meios que venham a ser empregados para propagar palavras e opiniões dos parlamentares. Precedentes. Possível aplicação da imunidade a manifestações em meios

> de comunicação social e em redes sociais. 4. Imunidade parlamentar. A vinculação da declaração com o desempenho do mandato deve ser aferida com base no alcance das atribuições dos parlamentares. As funções parlamentares abrangem, além da elaboração de leis, a fiscalização dos outros Poderes e, de modo ainda mais amplo, o debate de ideias, fundamental para o desenvolvimento da democracia Recurso Extraordinário com Repercussão Geral 600.063, Red. p/ acórdão Min. Roberto Barroso, Tribunal Pleno, julgado em 25.2.2015. 5. Imunidade parlamentar. Parlamentares em posição de antagonismo ideológico. Presunção de ligação de ofensas ao exercício das atividades políticas de seu prolator, que as desempenha vestido de seu mandato parlamentar; logo, sob o manto da imunidade constitucional. Afastamento da imunidade apenas quando claramente ausente vínculo entre o conteúdo do ato praticado e a função pública parlamentar exercida. Precedente: Inq 3.677, Red. p/ acórdão Min. Teori Zavascki, Tribunal Pleno, julgado em 27.3.2014. 6. Ofensas proferidas por senador contra outro senador. Nexo com o mandato suficientemente verificado. Fiscalização da coisa pública. Críticas a antagonista político. Inviolabilidade. 7. Absolvição, por atipicidade da conduta. (original sem destaques). (AO 2.002, Relator Min. Gilmar Mendes, 2ª Turma, DJE de 26.02.2016).

3.5 Rede Blockchain

Em recente decisão do Tribunal de Justiça de São Paulo, no âmbito de Agravo de Instrumento, o tema da validade jurídica das provas registradas em redes blockchain veio à tona. No processo de origem, as partes discutem a publicação indevida em redes sociais que teriam violado a honra e a imagem da vítima. Com o intuito de preservar as informações publicadas e garantir a comprovação das alegações no processo judicial, o autor efetuou registros das páginas *web* que continham os *posts* em rede blockchain, por intermédio de serviço prestado pela empresa Original My. A justiça entendeu ser o registro hábil a comprovar a veracidade e existência dos conteúdos, conforme trecho em destaque:

> OBRIGAÇÃO DE FAZER. TUTELA PROVISÓRIA DE URGÊNCIA. Publicações em páginas do Facebook, Instagram e Twitter. Alegação de conteúdos inverídicos e ofensivos, com o objetivo de produzir o descrédito do autor junto à opinião pública. Pretensão de remoção dos conteúdos, fornecimento de informações dos usuários e abstenção de comunicação dos requerimentos a terceiros. Descabimento. Requisitos do art. 300 do CPC ausentes. Liberdade de expressão e manifestação, direito à informação e inviolabilidade da honra e imagem assegurados pela Constituição Federal (arts. 5º, IX, IV, V e X, e 220). Controle judicial da manifestação do pensamento tem caráter excepcional, sob pena de indevida censura. Necessidade de demonstração da falsidade da notícia. Precedentes do STJ. Matéria fática que demanda análise mais aprofundada sob crivo do contraditório e ampla defesa. Ausentes requisitos necessários para o fornecimento liminar de informações dos usuários. Art. 22, Lei nº 12.965/14. Abstenção de comunicação a terceiros que não se justifica, pois o autor já providenciou a preservação do conteúdo. Decisão mantida. Recurso não provido. (TJ-SP - AI: 2237253-77.2018.8.26.0000 SP 2237253 – 77.2018.8.26.0000, Relator: Fernanda

> Gomes Camacho, Data de Julgamento: 19/12/2018, 5 Câmara de Direito Privado, Data de Publicação: 19/12/2018)

3.6 Manifestações Administrativas

O Tribunal de Contas da União, no acórdão nº 721/2019, proferido em 27/03/2019 pelo Plenário, defendeu, entre outras questões, o uso da tecnologia blockchain para a realização de procedimentos de contas. No caso concreto, no Processo nº TC 017.413/2017-6, de prestação de contas da ANCINE, o tribunal autoriza o prosseguimento de reuniões técnicas e de um projeto piloto para análise de viabilidade do uso da tecnologia nos processos de prestação de contas. A Corte destaca o potencial da tecnologia para aumentar a celeridade, a efetividade, a fidedignidade e a confiabilidade dos dados nas prestações de contas. Destaca-se trecho da decisão:

> 9.3.4. atente para o eventual emprego de novas tecnologias da informação, a exemplo do uso de blockchain, no bojo dos procedimentos de prestação de contas, com a subsequente análise dessas contas via robô virtual em prol do órgão federal repassador, podendo contribuir não apenas para a maior celeridade e efetividade no processo de prestação de contas dos repasses de recursos federais, mas também para a maior fidedignidade e confiabilidade das informações prestadas, de sorte a merecer os devidos estudos técnicos para o real desenvolvimento do aludido emprego, a partir da necessária implementação do correspondente projeto piloto para a efetiva aplicação dessas novas tecnologias da informação em determinado segmento de prestações de contas junto à Ancine, ficando autorizado, para tanto, que o Ministro-Relator dê prosseguimento às atuais reuniões técnicas entre o seu Gabinete e os dirigentes da Ancine, com a participação, entre outros, de unidades da secretaria do TCU e de representantes das eventuais instituições públicas e privadas, em face da apresentação do respectivo cronograma de atividades com o correspondente plano de ação para a referida implementação do projeto piloto. (Acórdão nº 721/2019 do Tribunal de Contas da União)

A Receita Federal, por meio da Portaria nº 1.788/2018, passou a adotar o compartilhamento de dados por meio de rede permissionada blockchain. O compartilhamento dos dados por meio da tecnologia deverá ser adotado a partir de 31 de julho de 2019. É válido ressaltar que a solução encontrada pela Receita Federal estabelece restrição para redes permissionadas. Ou seja, não é qualquer rede blockchain, mas apenas aquelas que possibilitam certo grau de controle, da Receita, por exemplo, para o credenciamento de usuários que terão acesso aos dados. É o que traz a Portaria:

> Art. 1º A Portaria RFB nº 1.639, de 22 de novembro de 2016, passa a vigorar com as seguintes alterações:
>
> Art. 6º A disponibilização de dados pela RFB ao órgão ou à entidade solicitante será operacionalizada, por qualquer meio ou solução que venha a ser adotada pela Cotec, no prestador de serviços de tecnologia da informação em que estejam localizadas as bases de dados da RFB, e somente será implementada com estrita observância do disposto nesta Portaria, na Portaria RFB nº 1.384, de 2016, e nas normas pertinentes à segurança da informação editadas pela RFB, mediante supervisão da Cotec.
>
> .....
>
> § 3º Fica autorizada a disponibilização de dados por meio de fornecimento de réplicas, parciais ou totais, até 31 de julho de 2019, período em que o órgão ou entidade solicitante deverá adotar o mecanismo de **compartilhamento de dados por meio de rede permissionada blockchain** ou outro autorizado pela Cotec. (NR)

O que se extrai das decisões dos órgãos federais acima é que a tecnologia blockchain tem grande potencial de uso para ampliar a transparência no Setor Público e conferir maior acessibilidade aos envolvidos nos processos. As primeiras iniciativas e os projetos piloto já estão em andamento e a tecnologia pode estar presente no Setor Público mais depressa do que se imagina.

4 LEGISLAÇÃO EM OUTRO PAÍSES

O desenvolvimento de aplicações em rede blockchain se difunde por vários países. Muitos projetos são desenvolvidos em parcerias de empresas espalhadas pelo mundo. O estudo sobre a legislação que está sendo atualizada em outros países e as percepções Governamentais sobre as redes blockchain podem ser de grande valia para auxiliar-nos na construção de um modelo brasileiro eficiente e que garanta o bom funcionamento dessas aplicações e a proteção de seus usuários e desenvolvedores.

Diante de uma compreensão jurídica e uma análise dos efeitos legais associados às redes distribuídas, faremos um estudo comparativo de como alguns países estabeleceram seus modelos de regulação.

Por exemplo, o estado de Delaware lançou uma iniciativa corporativa e está usando uma rede blockchain para registrar valores mobiliários do Uniform Commercial Code (U.C.C.) e outros documentos corporativos. A Estônia anunciou uma parceria com a BitNation para fornecer serviços de notarização baseados em blockchain, que concederá aos cidadãos estonianos a capacidade de registrar uma série de informações em uma rede blockchain, incluindo registros de casamento e certidões de nascimento.

Mais ambiciosamente, Dubai anunciou recentemente uma iniciativa liderada pelo governo que pretende ter todos os registros municipais armazenados e gerenciados por meio de uma blockchain até 2020. Iniciativas privadas estão preparadas para inspirar mais inovações governamentais, particularmente no contexto de propriedade intelectual e licenciamento. Plataformas como Ascribe e Monegraph usam rede blockchain para registrar as reivindicações de propriedade dos autores para obras protegidas por direitos autorais.

O MIT também lançou um projeto de certificados digitais, demonstrando como o blockchain poderia ser usado para emitir e verificar credenciais, que os governos poderiam generalizar para gerenciar esquemas de licenciamento estaduais. Esses usos emergentes, conforme explicam De Filippi e Wright (DE FILIPPI, WRIGHT, 2018), destacam as instâncias onde os governos poderiam confiar na tecnologia blockchain para manter registros importantes e informações do setor público de uma maneira mais descentralizada e resistente a falsificações.

4.1 Estados Unidos da América

O estado de Vermont adotou em 2016 explicitamente uma legislação que autoriza o uso de registros em blockchain como evidências de prova. Trata-se da lei **12 V.S.A. §1913**[23], que trata de questões relacionadas, entre outras coisas, a autenticação, a admissibilidade e a presunção de validade dos registros em blockchain.

O normativo define que o registro será considerado autêntico de acordo com a Lei de Evidências de Vermont 902 se estiver acompanhado de uma declaração de um especialista, feito sob juramento, alegando a qualificação daquela pessoa para certificar as informações especificadas pela lei. A conduta será considerada regular a não ser que a fonte de informação, ou método, ou circunstâncias de preparação indiquem falta de confiabilidade naquele registro.

A Lei presume que o registro verificado por meio de uma aplicação válida em blockchain será autêntico, que a pessoa que efetuou o registro será a pessoa responsável e que a presunção de validade não se estende ao conteúdo do registro.

Para maximizar a probabilidade de admissibilidade, o advogado que pretende utilizar uma evidência de blockchain deve considerar a legislação de Vermont, os objetivos da política de regras probatórias e o precedente Lizarraga-Tirado[24]. Cada uma dessas fontes sugere que o advogado deve estar preparado para reforçar suas evidências de blockchain com um testemunho de especialista. Para compilar uma descrição persuasivamente simples, porém tecnicamente sólida da tecnologia blockchain, os advogados precisarão desenvolver seus próprios conhecimentos de tecnologia blockchain e estabelecer relações com especialistas apropriados.

Observa-se que, embora alguns estados, como Arizona, Nevada e Delaware, aprovaram recentemente uma legislação que reconhece a legitimidade de contratos inteligentes garantidos por meio de tecnologia de blockchain, há um forte argumento de que a legislação atual, mais especificamente a ESIGN Act, que trata das assinaturas eletrônicas em relações comerciais nacionais e globais, e a UETA, que uniformiza transações eletrônicas entre 47 estados americanos, formam uma base legal suficiente para acolher os Smart Contracts de maneira eficiente, uma vez que esses contratos são eletronicamente assinados. [25]

---

[23] https://legislature.vermont.gov/statutes/section/12/081/01913. Acesso em: 22/04/2019.

[24] Foi um caso de condenação criminal em que o tribunal aceitou como meio de prova o registro de coordenadas de GPS no Google Earth, utilizados pela policial que efetuou a prisão do réu. https://law.justia.com/cases/federal/appellate-courts/ca9/13-10530/13-10530-2015-06-18.html

[25] Chamber of Digital Commerce, 'Smart Contracts' Legal Primer (https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf). Acesso em: 22/04/2019.

Como as leis existentes já fornecem uma base legal suficiente para a aplicação desses tipos de contratos, acreditamos que a legislação adicional **servirá apenas para criar leis estaduais inconsistentes, confundir o mercado e potencialmente atrapalhar a inovação**[26].

O tempo dirá se o Congresso ou a Suprema Corte modificarão as Regras Federais de Evidência para incluir uma solução uniforme para essas questões, ou se os tribunais abordarão essas questões de forma incremental à medida que surgirem. Também resta saber se outros estados seguirão a liderança de Vermont na adoção de regras que abordem essas incertezas das evidências. Enquanto isso, profissionais e profissionais devem considerar essas questões ao trabalhar com soluções baseadas em blockchain e litigar casos envolvendo registros blockchain.[27]

O estado de Delaware, também nos Estados Unidos, alterou a sua legislação que trata de registros de empresas e ações, Delaware General Corporation Law (DGCL), para expressamente autorizar que empresas utilizem redes ou bancos de dados distribuídos – blockchain – para criar e manter registros corporativos. A alteração surgiu de um contexto em que o processo de transferências de ações empresariais era muito burocrático e lento (dura cerca de 3 dias para que todas as partes validem a transação).

O parágrafo 224[28] da lei estabelece que esses registros eletrônicos serão válidos e admissíveis como evidências, e aceitos para todas as finalidades, equiparando-se para todos os efeitos aos registros do mesmo tipo de informação que estivessem registradas em papel.

---

[26] Chamber of Digital Commerce, 'Smart Contracts' Legal Primer (https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf)". Acesso em: 22/04/2019.

[27] https://www.law.com/newyorklawjournal/2018/12/14/blockchain-immutable-ledger-but-admissible-evidence/?slreturn=20190317201125

[28] Delaware - Section 1. Amend § 151(f), Title 8 of the Delaware Code – Senate Bill Nº 69

§ 224. Form of records

Any records maintained administered by a or on behalf of the corporation in the regular course of its business, including its stock ledger, books of account, and minute books, may be kept on, or by means of, or be in the form of, any information storage device, or method, or one or more electronic networks or databases (including one or more distributed electronic networks or databases), provided that the records so kept can be converted into clearly legible paper form within a reasonable time. Any corporation shall so, and, with respect to the stock ledger, that the records so kept (i) can be used to prepare the list of stockholders specified in § 219 and § 220 of this title, (ii) record the information specified in § 156, § 159, § 217(a) and § 218 of this title, and (iii) record transfers of stock as governed by Article 8 of subtitle I of Title 6. Any corporation shall convert any records so kept into clearly legible paper form upon the request of any person entitled to inspect such records pursuant to any provision of this chapter. When records are kept in such manner, a clearly legible paper form producedprepared from or by means of the information storage device or method shall be, method, or one or more electronic networks or databases (including one or more distributed electronic networks or databases) **shall be valid and admissible in evidence, and accepted for all other purposes, to the same extent as an original paper record of the same information would have been, provided the paper form accurately portrays the record**.

4.2 Reino Unido

O Governo do Reino Unido está desenvolvendo um projeto voltado para o registro de dados do Arquivo Nacional em uma rede blockchain. O objetivo do projeto é explorar o potencial de uso das redes distribuídas para manter confiança nos registros digitais.

O resultado final é a distribuição de várias cópias de um documento público que será registrado na rede com atributos de persistência e imutabilidade. Esse registro será verificável utilizando-se uma chave criptográfica que assegura a integridade do registro gravado na rede. A tecnologia pode alterar o futuro da gestão de arquivos e possibilitar uma difusão e compartilhamento entre diversos arquivos ao redor do mundo.[29]

Uma agência de defesa britânica, a Defense Advanced Research Projects Agency (DARPA), assinou um contrato de £ 1,8 milhões com a empresa Guardtime para investigar como o blockchain pode ser usado para fins de proteção militar. A empresa Guardtime utiliza tecnologia blockchain em conjunto com uma tecnologia Keyless Signature Infrastructure (KSI) para proteger usinas de energia nuclear e mecanismo de defesa contra inundações no Reino Unido.

4.3 China

A Suprema Corte da China entendeu serem válidas a utilização de evidências autenticadas via tecnologia blockchain em disputas legais. O novo entendimento da Corte surgiu em um contexto de esclarecimentos e maior transparência das regras de litígios resolvidos em Cortes Virtuais[30] no país e entra em vigor imediatamente.

A Corte declarou que "os tribunais da Internet devem reconhecer os dados digitais que são apresentados como evidência se as partes relevantes coletarem e armazenarem esses dados via blockchain com assinaturas digitais, registros de data e hora confiáveis e verificação de

[29] https://www.nationalarchives.gov.uk/documents/digital-projects-at-the-national-archives.pdf
[30] Em agosto de 2017, a cidade Hangzhou, na China, implementou a primeira corte eletrônica, que funciona em uma plataforma na internet e é voltada para a solução de litígios relacionados a internet. Beijing e Guangzhou também já possuem cortes virtuais.

valores de hash ou por meio de uma plataforma digital de depósito e comprovarem a autenticidade dessa tecnologia."[31]

As inovações relacionadas ao blockchain estão sendo legalmente reconhecidas como capazes de autenticar evidências e, além disso, como no caso dos Smart Contracts, têm o potencial de se tornarem uma enorme força disruptiva no meio jurídico. O imutável registrador de dados “carimbado” no tempo possibilita uma auditoria e verificação dos contratos com regras pré-estabelecidas.[32]

[31] www.court.gov.cn/zixun-xiangqing-116981.html. Acesso em: 23/04/2019.
[32]https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence

CONSIDERAÇÕES FINAIS

Preliminarmente, deve-se ressaltar que o objeto de estudo desse trabalho é relativamente novo no meio acadêmico, em especial na área do Direito. Isso significa que o maior acervo ainda são os recentes artigos acadêmicos das áreas da ciência da computação, da economia, da administração e do Direito. Os White-papers de implantação das redes blockchain também são importantes fontes de conhecimento para esse estudo. Por fim, a jurisprudência ainda não está consolidada sobre o tema e a grade maioria dos achados são casos que tangenciam o uso da tecnologia, a exemplo de fraudes com a emissão de criptomoedas, que, por vezes, sequer utilizavam uma rede blockchain para emissão.

Extraímos da primeira parte deste trabalho que a tecnologia possui três características predominantes que a tornam uma ferramenta de grande potencial de uso para aplicações em rede. São elas a imutabilidade, a integridade e a transparência. A partir dessa combinação, as aplicações distribuídas em rede blockchain dispensam a confiança em um ente central e passa a ser dependente de um consenso de rede. Ou seja, se os nós e mineradores que replicam os dados na rede são confiáveis, então os registros estarão protegidos e íntegros.

Algumas questões e incertezas ameaçam a plena confiança nas redes blockchain.

Muitas aplicações estão relacionadas a transferência de valores, criptomoedas ou *tokens*. Mesmo aquelas que não são precipuamente aplicações financeiras, tais como as aplicações de registros de imóveis ou de propriedade intelectual, muitas vezes demandam uma quantidade grande de transações por segundo. Algumas redes, tal como a Bitcoin, são ineficientes quanto ao número de transações que conseguem efetuar por segundo. A rede Lightning Network surgiu em 2017 com a intenção de resolver esse problema da Bitcoin e aumentar a capacidade de processamento.

Ainda relacionado ao problema de escalabilidade está o tamanho dos blocos que são armazenados e o tamanho de todo o conjunto de blocos que deverá ser armazenado na rede. A depender do tamanho do bloco definido por uma rede, permite-se uma maior ou menor quantidade de mineradores e de nós que irão replicar os dados. Isso significa que quanto maior o bloco for definido, possivelmente menos mineradores estarão vinculados à rede e, por

consequência, a rede estará mais concentrada nas mãos de poucos mineradores. Da mesma forma, se uma rede tem diversas finalidades de uso e seu volume de dados aumenta consideravelmente, então teremos uma situação indesejada de gasto de energia e dinheiro por parte de mineradores e nós para manutenção de uma rede com muito “lixo” digital.

As alterações das regras de consenso podem também ser um fator de ameaça à sobrevivência da rede. Se não houver um consenso e alguns mineradores optarem por não utilizar o novo script, então a rede poderá sofrer uma divisão (hard fork), e menos mineradores estarão envolvidos com a validação dos registros de cada lado remanescente. Outro problema dessa divisão da rede está vinculado a unicidade de registros. Em uma cadeia dominial de propriedade, não se pode admitir a possibilidade de uma bifurcação no histórico dos registros.

Quanto ao custo de operação da rede, deve-se levar em conta que ele é volátil e dependente da especulação da moeda virtual associada. Por exemplo, para realizar uma transação na rede Bitcoin, o usuário paga uma *fee* em bitcoins (btc), que oscila diariamente. Da mesma forma, uma transação em ethereum é paga em ether. A depender do tipo de transação que se deseja realizar, o custo pode ser proibitivo.

Algumas redes blockchain nasceram para a ser uma plataforma genérica, aberta para todo tipo de aplicação, enquanto outras redes, desde a concepção, buscaram a especialidade para um nicho de mercado. A flexibilidade da rede interfere diretamente na complexidade do conjunto de dados ou aplicação que será executada na rede DAO ou DAPP. A rede Bitcoin, por exemplo, efetua registros padrão com um campo “remetente”, um “destinatário”, um campo “valor” e um campo “extra”. O registro de uma transação que demande outros tipos de campos vai depender de uma camada de compatibilidade desenvolvida pelo provedor do serviço.

O anonimato nas redes também pode representar uma ameaça para situações em que é necessária a identificação do sujeito titular ou responsável pelo registro. Para as aplicações de propriedade intelectual, por exemplo, não faz sentido não saber a quem pertence aquele direito ou o correspondente registro.

Associado ao anonimato das redes está a dificuldade de responsabilização pelas falhas, fraudes ou danos gerados na rede. Sejam elas decorrentes do mau uso por usuários, de uma

falha de código por parte do desenvolvedor ou em razão exclusiva de ação de um haccker, a identificação de um responsável por danos é complexa e mecanismos que tentem mitigar esse problema correm um risco de inviabilizar o funcionamento da rede.

No intuito de delimitar um certo padrão seguro para o desenvolvimento de aplicações e serviços em plataformas descentralizadas blockchain, parece ser imprescindível a cooperação internacional. O desenvolvimento de padrões, limites e critérios mínimos de regulação são essenciais para minimizar os potenciais riscos dessas redes blockchain. É necessário haver uma harmonização entre as normas internacionais de responsabilização sobre essas redes mundiais, que envolvem o direito de muitos países simultaneamente.

Para a professora Cristie Ford (FORD, 2017), a regulamentação dessas novas tecnologias que inovam a forma como são prestados serviços e transacionados bens não pode ser rígida a ponto de inviabilizá-las. Na visão dela, uma regra rígida, além de inibir o desenvolvimento da inovação, não é suficiente para combater fraudes e comportamentos indesejados. Ela exemplifica com o caso do website Silk Road, que funcionou em 2013 transacionando bitcoin em troca de produtos ilícitos. Demonstra que, mesmo após o FBI interromper as operações do site, outras atividades ilícitas surgiram, sempre contornando as regras que estavam postas. Para a professora, uma regulamentação tem de ser flexível e entender as peculiaridades e os desafios da tecnologia, que ainda são pouco conhecidos.

> Considere o Bitcoin. Quando a criptomoeda foi lançada, seu status legal foi amplamente questionado. Esforços para banir a moeda foram em vão, entretanto, e a principal consequência foi a proliferação das diversas outras espécies de criptomoedas disponíveis. Esforços para interromper a operação do site da "dark web" Silk Road, no qual as transações eram realizadas em bitcoins, tiveram um efeito similar. O site tinha sido usado para negociar todos os tipos de itens ilícitos - particularmente drogas ilegais, que representavam cerca de 70% do mercado on-line. O FBI dos Estados Unidos fechou o website em outubro de 2013, mas apenas alguns meses depois, um website sucessor surgiu. Quando esse website, por sua vez, foi desativado, mais dois tomaram seu lugar. E desde que um desses websites deixou de funcionar, uma enorme quantidade de novos websites semelhantes surgiu. A tecnologia blockchain, na qual a criptomoeda se baseia, também parece ter um efeito muito mais perturbador sobre os serviços financeiros do que as próprias criptomoedas. A tecnologia de "smart contracts" que, indiscutivelmente, se torna possível, poderia prejudicar ainda mais as práticas profissionais em direito e contabilidade. (FORD, 2017)

Superadas a compreensão dos atributos das redes e os desafios associados, avançamos para o campo do direito a fim de estabelecer comparações e análises sobre os registros efetuados

em blockchain. À luz das fontes do Direito Brasileiro, parece ser razoável a equiparação dos registros eletrônicos ou contratos inteligentes efetuados em uma rede blockchain aos documentos eletrônicos.

O código civil e o Código de Processo Civil preveem a possiblidade de qualquer meio de prova moralmente legítimo. Os doutrinadores entendem que dentro do gênero de provas documentais está a espécie dos documentos eletrônicos. Em regra, encarados como documentos privados, produzidos por particulares e sem a fé pública dos documentos produzidos por agentes públicos.

Em 2001, a Medida Provisória nº 2.200-2/2001 estabeleceu uma série de regras concernentes a certificação digital tendo em vista a necessidade de adequação tecnológica do Direito. Era o início de uma era em que o documento público ou privado estaria cada vez menos em meio físico e sendo transformado para o meio digital.

Em 2006, o PJe, Processo Judicial eletrônico, ganhou força e atualmente é predominante na justiça Brasileira. Advogados, juízes e membros do Ministério Público assinam digitalmente as peças, que detêm o mesmo valor do papel.

O enunciado 297 da Jornada de Direito Civil estabeleceu que o documento eletrônico tem valor probante, contanto que se possa garantir a integridade e a autoria. Nessa linha, o STJ, em sede do RESP 1.495.920-DF, entendeu que o documento eletrônico tem valor de título extrajudicial. Da mesma forma que o Enunciado, a preocupação da Corte é quanto à integridade do conteúdo e à sua autoria.

Em 2016, o STJ reconheceu o valor probatório de correios eletrônicos trocados pelas partes em um suposto contrato que havia sido questionado em juízo. No mesmo ano, a Corte Superior também admitiu o uso dos “prints de tela” como meio de prova em processo judicial. Em ambos os casos, a preocupação quanto a autoria das mensagens é demonstrada pelas decisões.

Por fim, em 2018, o primeiro caso relacionado a validade jurídica de registros efetuados em rede blockchain foi decidido pelo STJ. Na decisão, os ministros entenderam ser válidos os registros com o fim de preservar as alegadas publicações ofensivas em redes sociais. Os registros dos *posts* em rede blockchain preservariam a integridade das provas na visão do Tribunal, que dispensou a necessidade de preservar de outra maneira o material no processo judicial.

Pode-se concluir que a legislação vigente é suficiente para permitir o desenvolvimento e a consolidação de aplicações com os mais diversos fins em blockchain. Na esteira do que foi proposto, os registros podem ser considerados para efeitos legais análogos aos contratos eletrônicos ou documentos digitais.

Estudos futuros poderão se debruçar sobre qual o conjunto de características mínimas desejáveis das redes para que sejam um ambiente seguro para o desenvolvimento de negócios jurídicos. Até o presente momento, é possível concluir que não basta dizer que qualquer registro em blockchain é seguro e goza automaticamente de uma validade jurídica. Deve-se considerar o tamanho da rede utilizada e a quantidade de mineradores, nós e participantes ativos. Ainda deve-se levar em conta o tipo de permissionamento da rede, o método de consenso, os critérios para atualização do método, a forma de incentivo à mineração, entre outros aspectos.

Todas essas questões serão determinantes para definir a integridade dos registros, a imutabilidade dos dados e a possiblidade de identificação e responsabilização das partes sempre que necessário. Por hora, cada caso deverá ser analisado pontualmente a depender da finalidade que se pretende.

O desenvolvimento de aplicações em blockchain pela Receita Federal, pelo Banco do Brasil, pelos órgãos do judiciário ou mesmo pelo Tribunal de Contas da União certamente contribuirá para uma melhor identificação dos ambientes mais seguros para a realização de transações virtuais em redes descentralizadas.

Eventualmente, redes próprias Governamentais serão desenvolvidas para servir de plataforma para soluções de serviços públicos. Ou, alternativamente, serão utilizadas redes já existentes abertas e públicas, mas com uma camada de proteção associada para conferir maior segurança jurídica. Apenas diante da necessidade será possível identificar o melhor caminho e o melhor tipo de rede para cada aplicação.

Os efeitos jurídicos vão depender de cada uma das escolhas que foram feitas. Em redes que detêm um permissionamento prévio, a responsabilização por falhas decorrentes da ação de intrusos na rede pode ser mais simples que em redes públicas abertas. Por outro lado, a publicidade de um dado transmitido fica prejudicada em redes privadas e, portanto, pode não ser desejável por aplicações que priorizam esse aspecto. Nota-se que as implicações jurídicas são decorrentes do tipo de rede que se adotou para cada solução.

REFERÊNCIAS BIBLIOGRÁFICAS

BECH, M. L., GARRATT, R. Central Bank Cryptocurrencies. **BIS Quarterly Review**, set. 2017. Disponível em: https://ssrn.com/abstract=3041906.

BÖHME, R., CHRISTIN, N., EDELMAN, B., MOORE, T. Bitcoin: Economics, Technology, and Governance. **Journal of Economic Perspectives**, 29, p. 213-238, 2015.

BONNEAU, J. et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. in: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2015.

BROWN, R. G. The Corda Platform: Na Introduction. 2018. Disponível em: https://docs.corda.net/_static/corda-platform-whitepaper.pdf

BUTERIN, V. Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. 2013. Disponível em: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

CÂMARA, A. F. **O Novo Processo Civil Brasileiro**. 5. ed. São Paulo: Atlas, 2019.

CATALINI, C., GANS, J. Some Simple Economics of the Blockchain. MIT SLoan School of Management Working Paper, 5191, 2016.

CHIU, J., KOEPPL, T. The Economics of Cryptocurrencies: Bitcoin and Beyond. Queen's University Working Paper, Canada, 2017.

COELHO, F. U. **Manual de direito comercial**: direito de empresa. 23. ed. São Paulo: Saraiva, 2011.

COMMITTEE ON THE GLOBAL FINANCIAL SYSTEM. Central bank operating frameworks and collateral markets. **CGFS papers**, 53, 2015.

DE FILIPPI, P., WRIGHT, A. **Blockchain and the Law**: The Rule of Code. Cambridge: Harvard University Press, 2018.

DIDIER Jr., Fredie. **Curso de direito processual civil v. 2**: teoria da prova, direito probatório, decisão, precedente, coisa julgada e tutela provisória. Salvador: JusPODIUM, 2015.

DOGUET, J. J. The nature of the form: legal and regulatory issues surrounding the bitcoin digital currency system. **Louisiana Law Review**, v. 73, n. 4, p. 1119-1130, 2013.

EUROPEAN CENTRAL BANK. **Virtual currencies schemes**: a further analysis. Frankfurt am Main: Eurosystem, 2015.

EVANS, D. Economic aspects of bitcoin and other decentralized public-ledger currency platforms. Coase-Sandor Institute For Law And Economics Working Paper, 685, 2014.

FARMER Jr., P. H. Speculative Tech: The Bitcoin Legal Quagmire & The Need for Legal Innovation. **Journal of Business & Technology Law**, 9, p; 85-86, 2014.

FORD, C, **Innovation and the State**: Finance, Regulation, and Justice. Cambridge: Cambridge University Press, 2017.

GARRATT, R., WALLACE N. Bitcoin 1, Bitcoin 2, ... : An experiment in privately issued outside monies. Department Of Economics University Of Santa Barbara Working Paper, 2016.

HEARN, M. Corda: a distributed ledger. 2016. Disponível em: https://github.com/corda/corda/blob/master/docs/source/_static/corda-technical-whitepaper.pdf.

KAPLANOV, N. M. Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. 2012.

KONING, J. Fedcoin. **Moneyness**, 19 out. 2014. Disponível em: http://jpkoning.blogspot.com/2014/10/fedcoin.html.

____. Fedcoin: a central bank issued cryptocurrency. **R3 Report**, 15 nov. 2016. Disponível em: https://static1.squarespace.com/static/.../R3+Report-+Fedcoin.pdf.

LAGO JR, A. **Responsabilidade civil por atos ilícitos na internet**. Editora LTR, 2001.

LÓSSIO, Cláudio. Blockchain e sua criptografia aliada a Segurança da Informação dos Cartórios. Disponível em: http://www.anoreg.org.br/site/2017/07/04/artigo-blockchain-e-o-cartorio-claudio-lossio/. Acesso em: 25 maio 2019.

LY, M. K. M. Coining Bitcoin's "LegalBits": Examining The Regulatory Framework for Bitcoin and Virtual Currencies. **Harvard Journal of Law & Technology**, v. 27, n. 2, p. 587-596, 2014.

MALEKAN, O. **The Story of the Blockchain**. New York: Triple Smoke Stack, 2018.

MARCACINI, A. T. R. O documento eletrônico como meio de prova. 1999. Disponível em: https://simagestao.com.br/wp-content/uploads/2016/05/Odocumentoeletronicocomomeiodeprova.pdf. Acesso em: 21/04/2019.

MARINONI, L. G., ARENHART, S. C. **Comentários ao código de processo civil**. São Paulo: Editora Revista dos Tribunais, 2016.

MARINONI, L. G., ARENHART, S. C., MITIDIERO, D. **Novo código de processo civil comentado I**. São Paulo: Editora Revista dos Tribunais, 2015.

MARQUES, A. T. G. L. **A prova documental na internet**. Curitiba: Juruá, 2005.

MEARLAN, L. Cinco problemas com o Blockchain que ainda precisam ser resolvidos. **CIO**, 7 jan. 2018. Disponível em: https://cio.com.br/cinco-problemas-com-o-blockchain-que-ainda-preciam-ser-resolvidos/.

MONETARY AUTHORITY OF SINGAPORE. **The future is here** – Project Ubin: SGD on distributed ledger. Cingapura: 2017.

MOUGAYAR, W. **Blockchain para negócios**: promessa, prática e aplicações da nova tecnologia da internet. Rio de Janeiro: Alta Books, 2017.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf.

NARAYANAN, A. *et al*. **Bitcoin and Cryptocurrency Technologies**. Princeton: Princeton University Press, 2016.

OSORIO JR, Edilson. Anonymous electronic voting system on public blockchains. 2018. Disponível em: https://github.com/eddieoz/haal/blob/master/whitepaper/Whitepaper%20-%20Anonymous%20Electronic%20Voting%20System%20on%20Public%20Blockchains.pdf

RASKIN, M., YERMACK, D. Digital currencies, decentralized ledgers and the future of central banking. NBER working papers, 22238, 2016.

SANTOS, M. A. **Prova judiciária no cível e comercial**. São Paulo: Max Limonad, 1970, v. 1, p. 55-56.

SCHWARTZ, D., YOUNGS, N., BRITTO, A. **The Ripple Protocol Consensus Algorithm**. Ripple Labs Inc., 2014. Disponível em: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

SNOW, P., DEERY, B., LU, J., JOHNSTON, D., KIRBY, P. Business processes secured by immutable audit trails on the blockchain. **Factom**, nov. 2014. Disponível em: https://raw.githubusercontent.com/FactomProject/FactomDocs/master/Factom_Whitepaper.pdf

SONG, W. Bullish on Blockchain: Examining Delaware's Approach to Distributed Ledger Technology in Corporate Governance Law and Beyond. **Harvard Business Law Review**, 2018.

STROMBERG, G. T. *et al*. Are Headwinds Hampering Delaware's Blockchain Initiative? **Law360**, mar. 2018. Disponível em: https://jenner.com/system/assets/publications/17844/original/stromberg%20Law360%20March%2023%202018.pdf?1521837416.

TAUBER, Nimrod. Blockchain and Evidence Law. Disponível em: https://www.legalbusinessworld.com/single-post/2018/12/17/Blockchain-and-Evidence-Law. Acesso em: 26 maio 2019.

TEMPELHOF, TEISSONIERE, TEMPELHOF, EDWARDS. Jurisdição Pangea e Pangea Arbitration Token (PAT): A Internet da Soberania. **Bitnation**, abr. 2017. Disponível em: THEODORO JR., H. Código de Processo Civil anotado. 21. ed. Rio de Janeiro: Forense, 2018.

ZETZSCHE, D. A., BUCKLEY, R. P., ARNER, D. W. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain (August 13, 2017). **University of Illinois Law Review**, v. 2018, n. 4, p. 1361-1407, 2018. Disponível em: https://ssrn.com/abstract=3018214.

WORLD ECONOMIC FORUM. Deep Shift Technology Tipping Points and Societal Impact. 2015. Disponível em: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso em: 29/05/2019